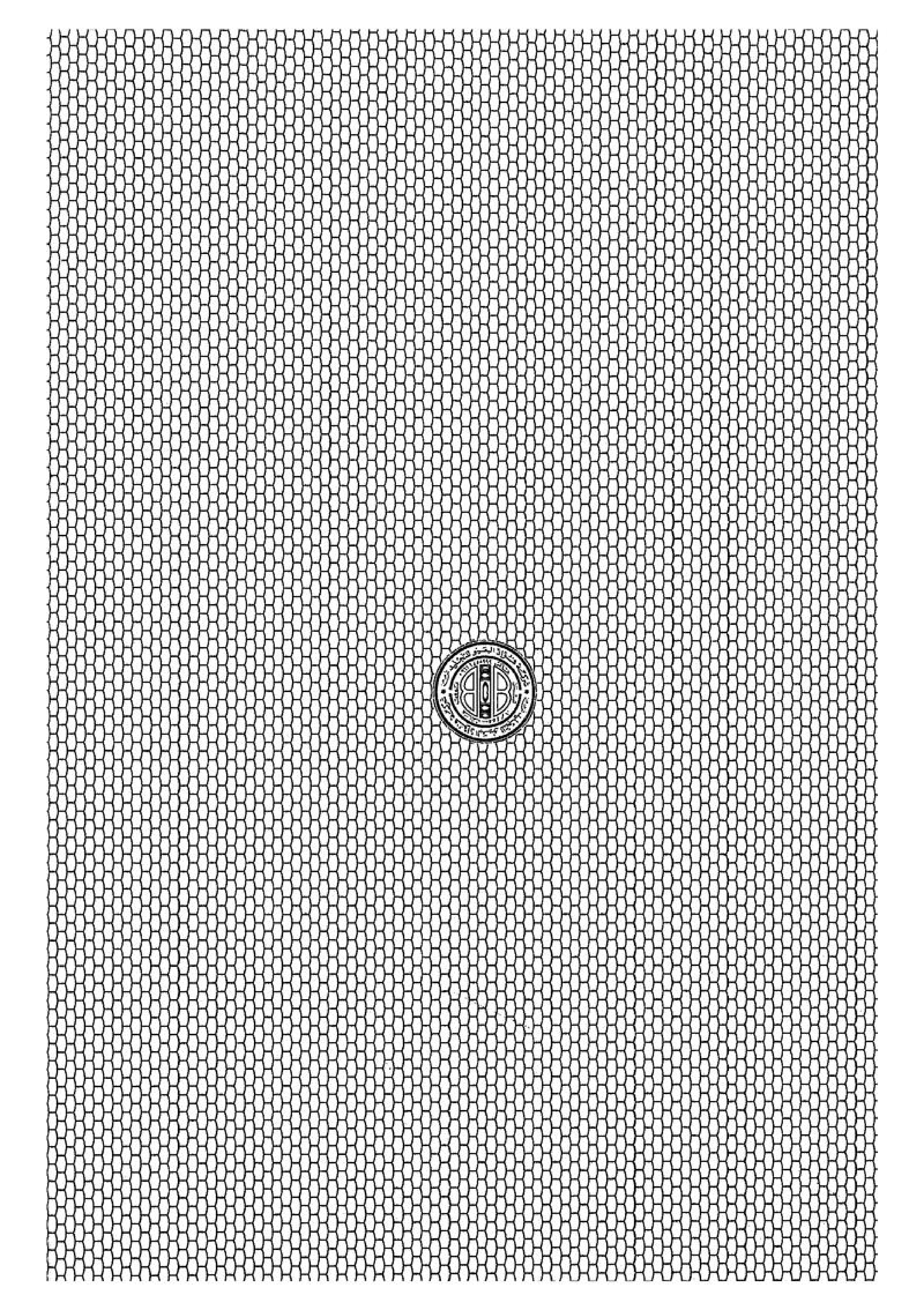
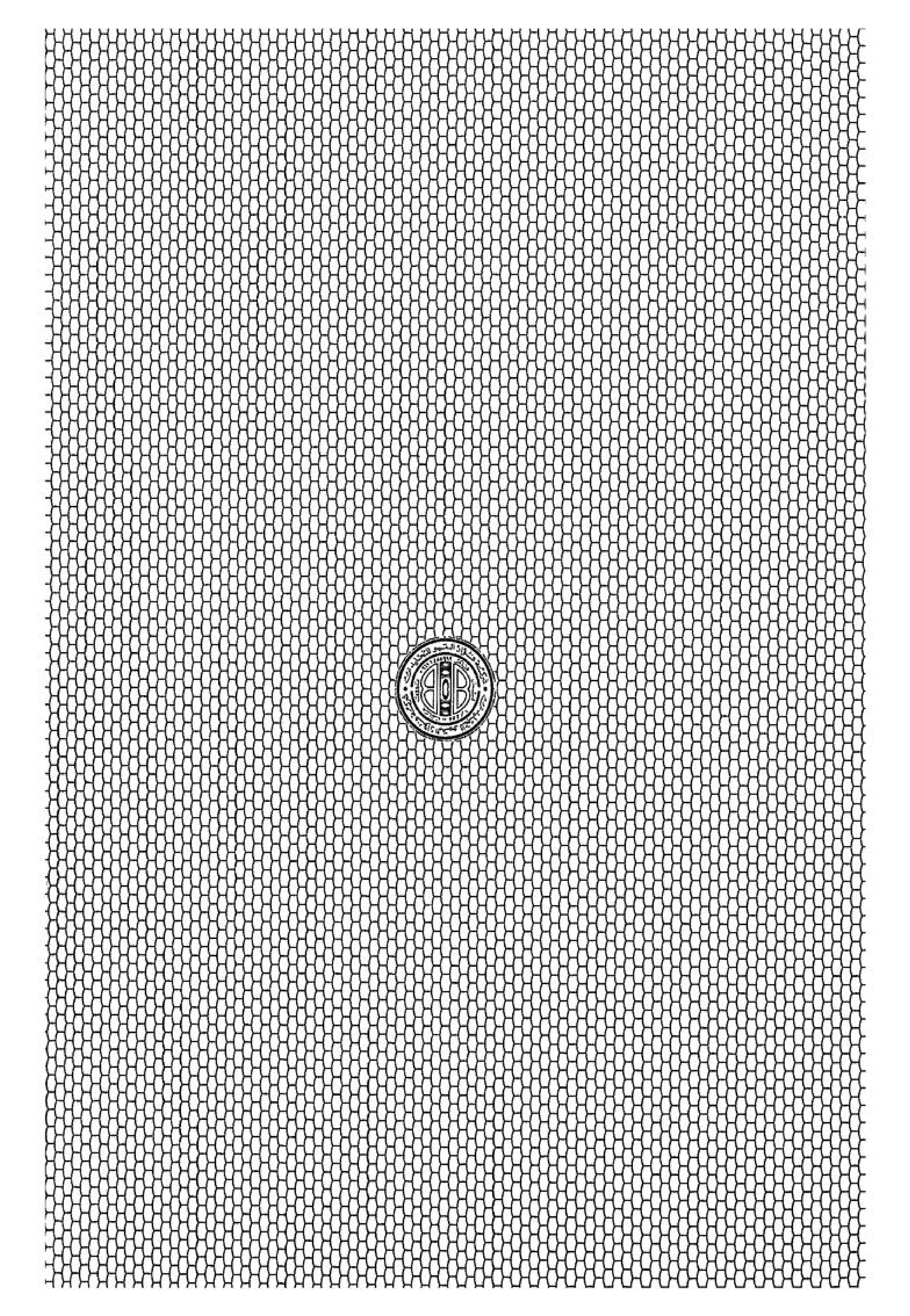
الجرائم المعلوماتية



نهلا عبد القادر المومني
ماجستير في القانون الجنائي المعلوماتي







المملكة الأردنية الهاشمية/رقم الإيداع لدى دائرة المكتبة الوطنية: (2007/4/1021)

346,048

المومني، نهلا عبد القادر

الجرائم المعلوماتية / نهلا عبد القادر

المومني - عمان: دار الثقافة 2010

رقم الإيداع: (2007/4/1021)

الواصفات: /الجرائم الحاسوبية//حماية

البيانات//شبكات المعلومات//السرية//

• أعدت دائرة المكتبة الوطنية بيانات الفهرسة والتصنيف الأولية

ISBN 9957-16-324-2

الطبعة الأولى 2008م - 1429هـ

الطبعة الثانية 2010م - 1431هـ



المركز الرئيسي: عمان - وسط البلد - قرب الجامع الحسيني - عمارة الحجيري

هاتف: 4646361 6 (962 +) فاكس: 4610291 6 (962 +) ص.ب 1532 عمان 11118 الأردن

فرع الجامعة: عمان - شارع الملكة رانيا العبدالله (الجامعة سابقاً) - مقابل بوابة العلوم - مجمع عربيات التجاري

هاتف: 5341929 6 (962 +) فاكس: 5344929 6 (962 +) ص.ب 20412 عمان 11118 الأردن

Website: www.daralthaqafa.com e-mail: info@daralthaqafa.com

تصميم وإنتاج

مكتب دار الثقافة للتصميم والإنتاج

الجرائم المعلوماتية

نهلا عبد القادر المومني
ماجستير في القانون الجنائي المعلوماتي

أصل هذا الكتاب (رسالة ماجستير)
بإشراف الدكتورة رنا العطور
في الجامعة الأردنية - الأردن



1431هـ-2010م

الإهداء

إلى . . .

والدتي . . . زهرة هذا العمر وشبابه

إلى . . .

تلك الإنسانة الراقية النبيلة التي أضاءت درب الحياة بعشقها الأبدي للتفاني والإخلاص

إلى . . .

من تقطن في مقلتيها أحلام الحاضر والغد . . .

إلى من ارتسمت في محياها أحلى وأعمق المعاني الإنسانية

إلى . . .

والدي . . . صاحب القلب الكبير

الذي علمنا أن تقوى الله رفيق صالح للعلم النافع والخلق الحسن

وأنهما يسيران معاً فيخلقان إنساناً يبني المجتمع ويعمّر هذه الأرض

إلى . . .

رفقاء الدرب . . . وأصدقاء الروح . . . أخواتي وإخواني

إليكم جميعا أهدي هذا الجهد العلمي

الفهرس

الفصل التمهيدي
الجانب الفني والتقني لجهاز الحاسوب وشبكة الإنترنت (النظام المعلوماتي)

الفصل الأول
ماهية الجريمة المعلوماتية وسماتها العامة

الفصل الثاني
الجرائم المعلوماتية الواقعة على النظام المعلوماتي

الفصل الثالث

الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

ملخص

تناولت هذه الدراسة موضوعاً حديثاً نسبياً هو موضوع الجريمة المعلوماتية في قانون العقوبات الأردني. وتهدف هذه الدراسة إلى التعرف على الجريمة المعلوماتية من حيث: ماهيتها وخصائصها وأهمية الحماية الجنائية للمعلوماتية من الجرائم التي قد تقع عليها، كما عمدت هذه الدراسة إلى تسليط الضوء على مرتكب هذه الجريمة الذي اصطلح على تسميته بالمجرم المعلوماتي، وذلك لمعرفة سماته وفئاته ودوافعه لارتكاب الجريمة المعلوماتية، حيث أن دراسة شخصية المجرم تعتبر خطوة هامة في وضع التشريعات العقابية التي تكفل إصلاحه وردعه في آن واحد.

وكان محور هذه الدراسة الأساسي هو البحث فيما إذا كانت النصوص التقليدية في قانون العقوبات الأردني يمكن أن تمتد لتشمل في إطارها الجرائم المعلوماتية المستحدثة التي قد يكون النظام المعلوماتي محلاً وموضوعاً لها أو التي قد ترتكب بواسطة هذا النظام. وقد اعتمدت هذه الدراسة على تحليل النصوص الجزائية الواردة في قانون العقوبات وذلك لمعرفة مدى انطباقها على الجرائم المعلوماتية.

ومن خلال هذا التحليل وجدنا أن هناك عقبات تحول دون تطبيق هذه النصوص التقليدية على الجرائم المعلوماتية. وأهم هذه العقبات هي أن نصوص قانون العقوبات وضعت ابتداءً لحماية الأموال المادية ذات الكيان المادي الملموس ولم توضع لحماية الأموال المعنوية كالمعلومات، حيث أن فكرة المال المعلوماتي لم تكن قد تبلورت لدى المشرع حين سنَّ هذا القانون وذلك لعدم اعتماد المجتمع على تكنولوجيا المعلومات في ذلك الوقت.

كما أن المبدأ الأساسي الذي يحكم القانون الجنائي هو مبدأ شرعية الجرائم والعقوبات، حيث لا جريمة ولا عقوبة إلا بنصٍ صريحٍ وكذلك عدم جواز التوسع في تفسير النصوص الجزائية يشكل عائقاً آخر أمام إمكانية إدراج الجرائم المعلوماتية ضمن النصوص التقليدية في قانون العقوبات الأردني.

وقد توصلت الدراسة إلى عدد من التوصيات منها: ضرورة تدخل المشرع الجزائي الأردني لتعديل النصوص الجزائية الواردة في قانون العقوبات حيث تراعي أيضا طبيعة المعلومات وخصوصيتها أو استحداث نصوص خاصة تكفل الحماية الجزائية للمعلوماتية. كما خلصت الدراسة إلى ضرورة تأهيل جهات الشرطة والادعاء العام والقضاء ليكونوا قادرين على التعامل مع هذا النوع المستحدث من الجرائم وذلك من خلال إعطائهم الدورات المتخصصة في هذا المجال. كما توصلنا أخيراً إلى أن التعاون الدولي هو مطلبٌ أساسيّ لمواجهة الجرائم المعلوماتية والتصدي لها.

مقدمة

1- يشهد العالم منذ منتصف القرن العشرين ثورة جديدة، اصطلح على تسميتها بالثورة المعلوماتية وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، فقد أمست قوة لا يستهان بها في أيدي الدول والأفراد. وكان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات و الاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة.

ومما لا شك فيه أن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها قد تركت آثاراً ايجابية وشكّلت قفزةً حضاريةً نوعيةً في حياة الأفراد والدول، حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظراً لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها بين الأفراد والجهات والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول. كما أصبحت هذه الأنظمة مستودعاً لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية والاقتصادية، كذلك أمست مستودعاً لأسرار الدول الحربية والصناعية والاقتصادية التي تعتبر على قدر من الأهمية والسرية.

2 ـ إلا أن هذا الجانب الإيجابي المشرق لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والمتمثلة في إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبصورة تضر بمصالح الأفراد والجماعات وبالتالي بمصلحة المجتمع كله، حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم اصطلح على تسميتها بالجرائم المعلوماتية.

وترتبط هذه الجرائم ارتباطاً وثيقاً بمدى اعتماد المجتمع بمؤسساته المختلفة الخاصة والعامة على الأنظمة المعلوماتية في إنجاز أعمالها، فكلما زاد الاعتماد على

هذه الأنظمة في القطاعات المختلفة زادت من فرص ارتكاب الجريمة المعلوماتية، خاصة في ظل تبني بعض الدول ومنها الأردن لمشروع الحكومة الإلكترونية الذي يهدف إلى تقديم جميع الخدمات إلى المواطنين إلكترونياً عن طريق استخدام الأنظمة المعلوماتية.

ولقد أدى ظهور الجرائم المعلوماتية إلى خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول وخاصة في مواجهة قانون العقوبات، الأمر الذي دعا الفقه والقضاء إلى البحث فيما إذا كانت النصوص القائمة كافية لمواجهة هذه الجرائم بشتى أنواعها أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها.

3 ـ وتعنى هذه الدراسة المتواضعة بتسليط الضوء على الجريمة المعلوماتية وتحديداً جرائم الحاسوب والإنترنت باعتبارها جرائم تتميز بالحداثة وذلك نظراً لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات الأمر الذي جعلها تتسم بمجموعة من الخصائص والسمات الخاصة.

كما سنحاول البحث في مدى كفاية القواعد القانونية التقليدية الواردة في قانون العقوبات الأردني وملاءمتها في الانطباق على هذه الجرائم المستحدثة. فالقاضي الجنائي ـ كما هو معروف ـ مقيد عند نظره للدعوى الجنائية بمبدأ شرعية الجرائم والعقوبات وبالتالي فإنه لن يستطيع تجريم أفعال لم ينص عليها المشرع حتى لو كانت هذه الأفعال تشكل انتهاكاً واضحاً لحقوق الغير وحرياتهم وكل ما يمكنه فعله هو محاولة تفسير النصوص المعمول بها والنظر فيما إذا كانت هذه السلوكيات المستحدثة تدخل ضمن إطار النص القانوني أم لا.

4 ـ ولقد وقع اختياري على دراسة موضوع الجريمة المعلوماتية بالرغم مما يكتنفه من صعوبات؛ إيماناً مني بأهمية الوقوف على هذا النمط المستحدث من الجرائم الذي بدأ يغزو مجتمعاتنا مع زيادة استخدام الأنظمة المعلوماتية مناحي الحياة كلّها.

وتتمثل أهم هذه الصعوبات في قلة المراجع المتوافرة في المكتبة العربية حول الجرائم المعلوماتية ، وكذلك ندرة التطبيقات القضائية في هذا المجال؛ نظراً لحداثة هذا الموضوع على الساحة القانونية العربية ولاتصاله كذلك بجانب تقني فني يتمثل بالنظام المعلوماتي بشقيه المادي والمعنوي. أضف إلى ذلك أن الجرائم المعلوماتية بصفة عامة لا يمكن حصرها ، فتكنولوجيا المعلومات متطورة ومتغيرة مما يؤثر بدوره على الجريمة المعلوماتية. كما أن الفقه حتى هذه اللحظة لم يتبن معياراً موحداً وثابتاً لتصنيف هذه الجرائم، فهناك جانب من الفقه صنفها إلى جرائم سلوك ونتيجة أولاً، وجرائم سلوك مجرد ثانياً، وجانب آخر صنّفها إلى جرائم تقع على الذمة المالية وأخرى تقع على الأشخاص، وآخرون صنفوها إلى جرائم يستخدم فيها النظام المعلوماتي وسيلة للاعتداء وأخرى يكون فيها النظام المعلوماتي محلا للاعتداء، وهو التصنيف الذي اعتمدناه في بحثنا المتواضع هذا.

5 ـ وقد ارتأيت تناول موضوع الجريمة المعلوماتية في قانون العقوبات الأردني في ثلاثة فصول يسبقها فصل تمهيدي. حيث نعرض في الفصل التمهيدي لمحة حول الجانب الفني والتقني لجهاز الحاسوب وشبكة الإنترنت.

أما الفصل الأول فقد تناول تعريف الجريمة المعلوماتية والسمات التي تتميز بها ، ودواعي الحماية الجنائية للمعلوماتية من الجرائم التي قد تقع عليها ، ويلقي الضوء على المجرم المعلوماتي: سماته وطوائفه ودوافعه لارتكاب هذه الجرائم.

أما الفصل الثاني فقد عرض لأبرز الجرائم المعلوماتية التي يكون النظام المعلوماتي فيها محلاً للاعتداء، وأما الفصل الثالث فقد تناول أبرز الجرائم المعلوماتية التي يكون النظام المعلوماتي فيها وسيلة للاعتداء.

وتجدر الإشارة أخيرا إلى أنني عرضت ـ وبشكل سريع ـ إلى بعض الأمثلة من القوانين التي سنتها الدول المتقدمة في مجال استخدام المعلوماتية لمواجهة الجرائم المعلوماتية بكافة أشكالها؛ وذلك للاستفادة من تجربتها في هذا المجال.



الفصل التمهيدي

الجانب الفني والتقني لجهاز الحاسوب وشبكة الإنترنت (النظام المعلوماتي)

الفصل التمهيدي
الجانب الفني والتقني لجهاز الحاسوب وشبكة الإنترنت
(النظام المعلوماتي)

6 ـ على الرغم من أن الجانب الفني والتقني قد يبدو بعيدا عن لغة القانون، إلا أنني وجدت انه من المستحسن أن استهل هذه الرسالة بفصل تمهيدي اعرض فيه للجانب التقني للنظام المعلوماتي وذلك لارتباط الجريمة المعلوماتية ارتباطاً وثيقاً به لإزالة الغموض وتوضيح بعض المصطلحات التقنية العلمية المرتبطة بتكنولوجيا المعلومات التي قد تمرّ معنا في الفصول المتقدمة من هذه الرسالة. وبناء على ما سبق سوف أتطرق للجانب التقني لجهاز الحاسوب ولشبكة الإنترنت وذلك على النحو التالي:

المبحث الأول: الجانب الفني والتقني لجهاز الحاسوب.

المبحث الثاني: الجانب الفني والتقني لشبكة الإنترنت.

المبحث الأول
الجانب الفني والتقني لجهاز الحاسوب

7 ـ دراسة الجريمة المعلوماتية تقتضي التطرق إلى الجانب الفني والتقني لجهاز الحاسوب[1] لفهم طبيعة عمل هذه التقنية الحديثة ومعرفة مكوناتها المادية والمعنوية.

المطلب الأول: تعريف الحاسوب وخصائصه

8 ـ يعرف الحاسوب بأنه: "عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية هي: استقبال البيانات المدخلة (الحصول على الحقائق المجردة)، ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات)، وإظهار المعلومات المخرجة (الحصول على النتائج)"[2].

ونظام الحاسوب يمكن تعريفه أنه: "مجموعة من الأجهزة المترابطة والتي تعمل معاً من خلال مجموعة من الأوامر والبيانات لتحقيق حل لمسألة معينة"[3]. أو أنه: "مجموعة من أجهزة إلكترونية تقوم بصورة أوتوماتيكية باستقبال البيانات وخزنها ومعالجتها واستخراج النتائج تحت سيطرة تعليمات مخزنة فيها"[4].

---

(1) الحاسوب هي الترجمة التي اعتمدها مجمع اللغة العربية للكلمة الإنجليزية (Computer) وما يقابلها بالفرنسي (Ordinateur).

وبناء عليه ستستخدم الباحثة تعبير الحاسوب. كما أنه تجدر الإشارة إلى أن الجيل الخامس من أجهزة الحاسوب الحالية تعمل بالذكاء الاصطناعي وبالتالي لا حاجة لاستخدام كلمة آلي بعد كلمة حاسوب. انظر، لطفي، محمد حسام. الحماية القانونية لبرامج الحاسب، (ط1)، بحث منشور ضمن كتاب الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف، اتحاد المصارف العربية بيروت 1991، ص 73.

(2) الزعبي، محمد والشرايعة، احمد وقطيشات، منيب والفارس، سهير والزعبي، خالدة. الحاسوب والبرمجيات الجاهزة، ط1، دار وائل للنشر والتوزيع، عمان، 2002، ص 5.

(3) القاضي، زياد. أساسيات علم الحاسوب، ط1، صفاء للنشر والتوزيع، عمان، 1997، ص 13.

(4) الفخري، عوني. المسؤولية المدنية الناشئة عن استعمال الحاسوب. ورقة عمل مقدمة إلى ندوة القانون والحاسوب المنعقدة في العراق آب (1998)، بيت الحكمة، بغداد، ص 71.

9ـ ويطلق على مجموعة الأجهزة التي تشكل الكيان المادي الملموس لنظام الحاسوب لفظ (Hard ware) أي المعدات. ويطلق على مجموعة الأوامر أو التعليمات لفظ (Soft ware) أي البرمجيات.

وهذه المعدات والبرمجيات لا قيمة لها دون وجود المستخدمين، وهم الأشخاص الذين يتعاملون مع البرمجيات تحقيقاً لأهداف خاصة بهم تختلف من مستخدم إلى آخر.

أقسام الحاسبات الإلكترونية من حيث وظيفتها وتركيبها:

10ـ وتتنوع الحاسبات الإلكترونية حيث يمكن تقسيمها من حيث وظيفتها وتركيبها إلى:

أولاً: الحاسوب القياسي (Analog)

يستخدم هذا الحاسوب في القياسات الكمية التي لا يمكن التعبير عنها بالعدد مباشرة[1].

ثانياً: الحاسوب الرقمي (Digital)

الحاسوب الرقمي يتعامل مع الأرقام في عمليات الإدخال والإخراج والمعالجة فالبيانات تخزن في ذاكرته في شكل أرقام وإذا طلب منه استرجاعها فسيعطيها في الشكل المقروء وليس كما هو مسجل في ذاكرته، وهذا النوع هو المستخدم والمنتشر عالمياً في بنوك المعلومات[2].

ثالثاً: الحاسوب الهجين أو المختلط (Hybrid)

وهو الحاسوب الذي يجمع بين الأسلوبين السابقين. ويمكن الحصول عليه بالتوصيل المباشر بين حاسوب رقمي وآخر قياسي بواسطة جهاز تخزين خاص[3].

---

(1) مجالات استخدام هذا الحاسوب تكون في التطبيقات التي تحتاج إلى عمليات تفاضلية، وفي تطبيقات التغذية العكسية، إذ يستخدم في السيطرة على حركة القذائف الصاروخية والعمليات الكيماوية المسيرة بصورة أوتوماتيكية، وفي التطبيقات التي تحتاج إلى سيطرة آنية ومباشرة، وتستخدم أيضا في محطات توزيع الشبكات الكهربائية على المدن وفي شبكات الري الخارجية وفي سدود المياه.انظر، الفخري. مرجع سابق، ص 72.

(2) قشقوش، هدى. جرائم الحاسب الالكتروني في التشريع المقارن، ط1 ، دار النهضة العربية، القاهرة، 1992، ص19.

(3) الفخري، مرجع سابق، ص 72.

أقسام الحاسبات الإلكترونية من حيث أحجامها:

11ـ وتتنوع الحاسبات الإلكترونية كذلك من حيث أحجامها حيث يمكن تصنيفها من حيث الأحجام إلى:

أولا: الحاسوب الكبير (Mainframes)

ويتميز هذا الحاسوب بكبر حجمه وسعة ذاكرته والقدرة الفائقة على معالجة البيانات بسرعة عالية. وينفذ هذا الحاسوب ملايين التعليمات في الثانية الواحدة[1].

ثانيا: الحاسوب المتوسط (Mini Computer)

وهو حاسوب صغير نسبياً إذا قورن بالحاسوب الكبير. وهو ينجز عملياته بصورة متكاملة ووقت أطول من الوقت الذي ينجز فيه الحاسوب الكبير هذه العمليات[2].

ثالثاً: الحواسيب الصغيرة (Personal Computer)

وهو أصغر أنواع الحواسيب و أكثرها شيوعا. ويفضل الملايين من الأشخاص استخدامها نظراً لحجمها الصغير وتكلفتها المتدنية[3].

---

(1) الحواسيب الكبيرة تستخدم في الغالب الأعم من قبل البنوك والمنظمات الكبيرة لمعالجة كميات كبيرة من البيانات كتحضير الشيكات المدفوعة والفواتير والطلبيات. أنظر، الزعبي وآخرون، مرجع سابق، ص6. وكذلك الفخري، مرجع سابق، ص 72.

(2) تستخدم الحواسيب المتوسطة في الأعمال التجارية الكبيرة والمعقدة نوعاً ما. وتستخدم في الأماكن التي يكون فيها استخدام الحواسيب الشخصية غير مناسب. الفخري، مرجع سابق، ص 72، 73.وأنظر، كذلك الزعبي وآخرون، مرجع سابق، ص 6،5.

(3) الحواسيب الكبيرة والمتوسطة والصغيرة هي أشهر أنواع الحواسيب من حيث الحجم وهناك أنواع اخرى نذكر منها:

- الحواسيب المحمولة (Laptop Compute)، وهي حواسيب شخصية بحجم حقيبة اليد يمكن نقلها من مكان لآخر بمنتهى السهولة وهذه الحواسيب اغلى ثمناً نظراً لإمكانية نقلها.
- حواسيب الجيب (Palmtop Computer) وهي حواسيب صغيرة تمسك باليد وتقوم بالوظائف نفسها التي يمكن أن تقوم بها الحواسيب المحمولة ولكن بشكل أبسط.
- شبكات الحواسيب (Computer in Net works) وهي إما:

أ- مجموعة حواسيب شخصية تتصل معاً بأسلاك حيث يسهل نقل المعلومات بين الأجهزة، ولكن هذا لا يلغي استقلالية كل حاسوب عن الآخر بمعداته وبرمجياته.

ب- أو حاسوب يسمى الخادم (Server) يتصل مع مجموعة محطات أو طرفيات مثل الحواسيب الشخصية تسمى العملاء (Clients) .انظر، الزعبي وآخرون، مرجع سابق، ص 7، 8.

12- ومما يدعو إلى الدهشة حقاً هو حجم الثورة في مجال صناعة الحواسيب وما يرتبط بها من تقنيات، حيث أنها تتطور بشكل لم يسبق للإنسانية أن عاصرته أو حتى حلمت به، حتى إنه ليقال:

"لو أن صناعة السيارات والطائرات قد تطورت مثل تطور صناعة الحواسيب فإن تكاليف سيارة (الرولز رويس) يمكن أن تكون فقط (2.75) دولار أمريكي، وتسير ثلاثة ملايين ميل على جالون واحد من البنزين، وان تكاليف طائرة (البوينج 767) يمكن أن تبلغ خمسمائة دولار أمريكي وستدور حول العالم عشرين مرة على خمس جالونات بنزين"[1].

13- يمتاز الحاسوب بعدة خصائص ومميزات جعلت منه مادة رئيسية في حياتنا، وهي:

1- السرعة، إذ إنه يقوم بوظائفه بسرعة مذهلة مقارنة بسرعة البشر في معالجة البيانات وأداء الوظائف والقيام بالعمليات الحسابية. وهذه الخاصية توفر على الإنسان الكثير من الوقت الذي كان سيمضيه في إجراء العمليات الحسابية والمنطقية[2].

2- تخزين المعلومات واستعادتها حيث يتمتع الحاسوب بالقابلية لتخزين كمية هائلة من المعلومات والبيانات، حيث يمكن الرجوع إليها واستعادتها والاستفادة منها في أي وقت يحتاج إليها الإنسان وتبقى هذه المعلومات مخزنة لفترة طويلة جداً دون أن يحدث لها أي تغيير[3].

---

(1) فوريستر، توم. مجتمع التقنية العالية، (ترجمة محمد كامل عبد العزيز)، ط1، مركز الكتب الأردني، عمان، 1989، ص 35.

(2) تقاس سرعة انجاز الحواسيب للعمليات المختلفة عادة بالمايكرو ثانية اي (1 / مليون من الثانية) واحيانا بأجزاء المايكرو ثانية

(النانو ثانية 1 / بليون من الثانية). انظر، الغريب، انتصار، أمن الكمبيوتر والقانون، ط1، دار الراتب الجامعية، بيروت، 1994، ص20.

(3) المصدر السابق، ص 20، 21.

3- الدقة المتناهية في النتائج التي يخرجها الحاسوب، فإذا كانت المعلومات والبيانات المقدمة للتنفيذ صحيحة فإنه ليس هناك من سبب لقيام الحاسوب بإعطاء نتائج خاطئة. فالنتائج التي يخرجها الحاسوب هي نتائج دقيقة جداً.

4- قابلية الحاسوب للبرمجة، إذ يمكن تصميمه وتأهيله ليؤدي وظائف معينة وذلك عن طريق البرمجيات التي يمكن تطويرها وتطويعها لتؤدي وظائف لا حدود لها.

5- إمكانية التعامل مع الحاسبات الالكترونية عن بعد، ومن أي مكان في العالم عن طريق وسائل الاتصال السلكي واللاسلكي،[1] وعن طريق شبكات الحواسيب المعلوماتية، فهناك تعاون وتكامل في العلاقة بين تكنولوجيا المعلومات وتكنولوجيا الاتصالات.

هذه أهم المزايا الكثيرة التي يتمتع بها الحاسوب التي فتحت آفاقاً واسعة أمام البشرية للابتكار والاختراع ولكنها في ذات الوقت فتحت باباً واسعاً أمام الأشخاص ذوي المصالح الضيقة وأصحاب الغايات غير المشروعة.

المطلب الثاني: مكونات الحاسوب

14- يتكون نظام الحاسوب من قسمين رئيسيين هما المكونات المادية (Hardware) والمكونات المنطقية (Soft ware).

15- اولاً: المكونات المادية للحاسوب (Hard ware)

وتمثل هذه المكونات: الهيكل المادي أو الجسم المادي لنظام الحاسوب، ويتكون هذا الهيكل من الوحدات الرئيسية التالية:

(1) الحفناوي، فاروق، موسوعة قانون الكمبيوتر ونظم المعلومات، (ط1)، دار الكتاب الحديث، القاهرة، 2001، ص 30.

1- وحدات الإدخال (In put Units):

وتستعمل هذه الوحدات لإدخال المعلومات أو المعطيات أو البرامج المراد معالجتها من الوسط الموجودة عليه إلى ذاكرة الحاسوب. وتكون وسائل الإدخال على أنواع[1]:

- وسائل تسمح بالاتصال المباشر ON-LINE بين الإنسان "الوسط الخارجي" وبين وحدة المعالجة المركزية، وتمثل لوحة المفاتيح[2] إحدى هذه الوسائل حيث يتم إدخال المعلومات من خلال المفاتيح مباشرة إلى وحدة المعالجة المركزية.
- وسائل تسمح بإدخال المعلومات بصورة غير مباشرة OFF - LINE ويتم بهذه الوسائل تهيئة المعلومات المراد إدخالها على وسائط معينة ومحددة بمعزل عن الحاسوب أول الأمر ثم تتم عملية الإدخال من خلال عملية وحدة إدخال ملائمة إلى وحدة المعالجة المركزية.

وتشمل وحدات الإدخال كذلك الفأرة (Mouse) و كرة المسار (Track ball) ومشغلات الأقراص والماسح (Scanner).

2- وحدة المعالجة المركزية (Central Processing Unit):

وتشتهر بين مستخدمي جهاز الحاسوب باسمها المختصر(CPU). وتعتبر هذه الوحدة هي بمثابة العقل المفكر والمسيطر على عمل باقي الوحدات المكونة لجهاز

---

(1) الغريب، مرجع سابق، ص 16.

(2) تعتبر لوحة المفاتيح وحدة الإدخال الرئيسية في الحاسوب الأكثر انتشاراً وهي تماثل الآلة الكاتبة من حيث توزيع الحروف. وبعض لوحات المفاتيح تحتوي على أقل من ستين مفتاحاً وبعضها الآخر يزيد على ذلك. وهناك مفاتيح تؤدي وظائف خاصة مثل End , Home وهي المفاتيح التي تسمح بالانتقال إلى أول الشاشة أو إلى آخرها، ومفاتيح Pg dn , Pg up والتي تسمح بالانتقال إلى صفحة أعلى وصفحة أسفل، ومفتاح Prtse الذي يسمح بطباعة محتويات الشاشة. كما أن هناك مفاتيح الوظائف Functions Keys والتي تؤدي وظائف خاصة تتوقف على البرنامج التطبيقي المستخدم، وفي بعض لوحات المفاتيح تكون هناك أعداد إضافية Key Pad ، كما يوجد نوع من لوحات المفاتيح تسمى لوحة المفاتيح الحساسة للمس Touch Sensitive Key boardوهي لا تحتوي على مفاتيح متحركة ولكن عن طريق لمس مكان المفتاح فقط يتم توصيل إشارة كهربائية لإدخال الحرف المطلوب وهي تمتاز بعدم وجود فراغات وتستخدم مع العديد من أجهزة الحاسبات الصغيرة. انظر، محمود، عبد الله حسين علي. سرقة المعلومات المخزنة في الحاسب الآلي، ط1 ، دار النهضة العربية، القاهرة، 2002، ص 21، 22.

الحاسوب. وتقوم هذه الوحدة بمعالجة البيانات حسب التعليمات الواردة في البرنامج، حيث يتم فيها جميع العمليات الحسابية أو المنطقية. وتتكون هذه الوحدة من وحدتين رئيسيتين:

أ- وحدة التحكم والسيطرة (Control Unit):

وهي عبارة عن دوائر إلكترونية تتحكم في عمليات تنفيذ التعليمات وفي عمليات الإدخال والإخراج والتخزين والمعالجة داخل الحاسوب[1].ويمكن القول إن وحدة التحكم والسيطرة تقوم بالوظائف التالية[2]:

1- التنسيق والتحكم في البيانات الداخلة والخارجة من والى الذاكرة الرئيسية للحاسوب بتوجيهها إلى القنوات المختلفة.
2- تعتبر وسيلة اتصال من الذاكرة الرئيسية ووحدة الحساب والمنطق إلى باقي وحدات الحاسوب.
3- تحتوي على ساعة منطقية تقوم بالتحكم في توقيت العمليات المختلفة.
4- قراءة وتفسير تعليمات البرامج.

ب- وحدة الحساب والمنطق (Arithmetic Logic Unit):

والمعروفة اختصارا ب (ALU) وتقوم هذه الوحدة بجميع العمليات الحسابية والمنطقية، مثل المقارنات التي تسمح للحاسوب بتقييم المواقف لتحويلها إلى الذاكرة أو إخراجها حسب الطلب إلى وسط مناسب للمستخدم[3].

3- وحدة الذاكرة (Memory Unit):

وهي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو تخزين النتائج الآتية من وحدة المعالجة المركزية. وهناك نوعين من وحدات الذاكرة هما:

---

(1) الدريني، محمد، مقدمة في أساسيات الحاسوب، ط1، معهد الإدارة العامة، المملكة العربية السعودية، 1961 ص12.

(2) محمود، مرجع سابق، ص 20 . كذلك انظر، الزعبي وآخرون، مرجع سابق، ص 13، 14.

(3) منصور، عوض، برمجة الحاسبات الإلكترونية بلغة بيسك، ط1، دار الفرقان للنشر والتوزيع، عمان، 1986، ص4.

أ- وحدة الذاكرة الرئيسية (Main Memory):

وتستخدم هذه الوحدة لتخزين المعطيات والبرامج التي يراد تنفيذها وهي تتلاشى بمجرد الانتهاء من تنفيذ البرامج. وتختلف سرعتها من جهاز حاسوب لآخر، كما يمكن تغييرها للجهاز الواحد بأخرى أسرع منها وأقدر على استيعاب معلومات أكثر[1] .وتقسم هذه الذاكرة إلى قسمين:

1- ذاكرة القراءة فقط (Read Only Memory): والمعروفة اختصاراً بـ (Rom)، ومحتويات هذه الذاكرة من أوامر تكون مخزنة في الجهاز من قبل الجهة المصنعة له للقراءة فقط، بحيث لا يمكن للمستخدم التعديل عليها. ومن خصائص هذه الذاكرة: الاحتفاظ بالبيانات والأوامر المخزنة حتى بعد انقطاع التيار الكهربائي، وكما أنها لا تقبل تخزين أي بيانات بعد تصنيعها إلا بمعرفة الجهة الصانعة أو المتخصصين باستخدام أجهزة خاصة. وهذه الذاكرة تستخدم بصفة عامة لقراءة البيانات الموجودة بها فقط.

2- الذاكرة العشوائية أو ذاكرة الوصول العشوائي (Random Access Memory): والمعروفة اختصار بـ (RAM) وهذه الذاكرة تخزن فيها البيانات بصورة مؤقتة استعداداً لمعالجتها أو لتخزينها في وسائط التخزين الدائمة. وهذه الذاكرة تحفظ جميع الملفات الرئيسة للبرامج عند البدء بتشغيلها؛ لذلك فإن حجم أو سعة هذه الذاكرة من العوامل الرئيسة التي تؤثر على مدى فعالية الجهاز، فبعض البرامج تحتاج إلى ذاكرة عالية لتشغيلها وبغير ذلك يكون من الصعب استخدامها.

ب- وحدة الذاكرة المساعدة (Auxiliary Memory):

تعتبر هذه الوحدة وحدة ثانوية لتخزين المعلومات والبرامج[2] إذا ما قيست بالوحدة الرئيسة؛ لذا فإنها تكون أرخص ثمناً وأقل سعةً منها، إلا أنها تحتفظ

(1) المصدر السابق، ص 4.

(2) اهمية الذاكرة الثانوية تظهر في تخزينها لمجموعات من البيانات تحتاج لأن تحفظ بعيداً عن ذاكرة الحاسوب الرئيسة، وهذه المجموعات تعرف بالملفات (Files) وتمتاز بحجمها الكبير وديمومتها. انظر، الزعبي وآخرون، مرجع سابق، ص28 .

بالمعلومات فيها لمدة طويلة قد تصل عدداً من الأعوام وذلك لأنها تستعمل أقراصاً أو اسطوانات مغناطيسية.

وهناك عدة أنواع للذاكرة الثانوية منها: الأقراص المرنة والأقراص الصلبة والأشرطة الممغنطة والقرص الضوئي والقرص الرقمي.

4- وحدات الإخراج:

وحدات الإخراج تؤدي مهمة إيصال الحاسوب بالوسط الخارجي، فمهمتها هي عكس مهمة وحدات الإدخال التي كانت واسطة اتصال الوسط الخارجي بالحاسوب.

والوسط الخارجي في الحالتين في معظم الأحيان يتمثل بالإنسان المستخدم للحاسوب. فوحدات الإخراج تقوم بنقل النتائج المستخرجة من حل أو معالجة مسألة معينة من وحدة المعالجة المركزية إلى الخارج[1]. وتتمثل أهم وحدات الإخراج فيما يلي:

أ- الشاشة (Screen):

تعد الشاشة من أهم وحدات الإخراج فمن خلالها يتمكن المستخدم من مشاهدة نتائج ما قام به من أعمال (أوامر كانت ونصوصاً مدخلة) أو مشاهدة نتائج البيانات بعد أن يتم معالجتها داخل جهاز الحاسوب.

ب- الطابعة (Printer):

بعد الشاشة، فإن الطابعة تعتبر من وحدات الإخراج الأكثر استعمالا ويتم من خلالها تزويد المستخدم بنسخ مطبوعة من البيانات والنتائج المخزنة داخل جهاز الحاسوب.

16- ثانياً: المكونات المنطقية لجهاز الحاسوب (Soft ware)

وتتمثل هذه المكونات المنطقية بالتطبيقات العملية التي تجرى داخل الكيان المادي للحاسب. والمكونات المنطقية تشمل بالإضافة إلى المعلومات والبيانات برمجيات الحاسوب.

(1) الغريب، مرجع سابق، ص17.

واصطلاح برمجيات الحاسوب (Computer Software) اصطلاح أعمُّ وأشمل من تعبير برنامج الحاسوب[1] (Computer Program)، إذ يدخل في مفهوم برمجيات الحاسوب أمور أخرى غير البرنامج وان كانت وثيقة الصلة به، مثل: الوثائق والمستندات والمواد التي يطلق عليها المواد المساندة (Supporting Material)، وهي مواد مكتوبة في صورة كتيبات أو منشورات تطبع حالياً على الوسائط الإلكترونية مثل الأقراص المرنة أو الأقراص المدمجة، ومهمتها شرح البرنامج وتيسير فهمه ومساعدة مستعمليه على كيفية تشغيله ويطلق على هذه المواد كتيب إرشادات الاستعمال. ويدخل ضمن تعبير البرمجيات كذلك كل الوثائق والمستندات التي تنتج في مرحلة تصميم البرنامج وتطويره[2].

أما برنامج الحاسوب فهو مجموعة من الأوامر والإرشادات والايعازات التي تحدد لجهاز الحاسوب العمليات التي يقوم بتنفيذها بتسلسل وخطوات محددة، وتحمل هذه العمليات على وسيط (Media)[3] معين يمكن قراءته عن طريق الآلة وبعد ذلك يمكن للبرنامج عن طريق معالجة البيانات أن يؤدي وظائف معينة ويحقق النتائج المطلوبة منه[4].

أنواع البرمجيات:

وهناك نوعان من البرمجيات:

---

(1) تعبيرا البرمجيات Software والبرنامج Porogram كثيراً ما يختلط في الحياة العملية، فيطلق احد التعبيرين ويقصد به الآخر والبرنامج عموما تعبير عام قد يقصد به حزمة برامج Software Packge وهي مجموعة برامج متكاملة يطرحها منتجوها في الأسواق باعتبارها منتج واحد رغم انها تتضمن أكثر من برنامج، ومثال هذه الحزم، الحزمة المشهورة (Micro Soft Office). انظر، الحفناوي، مرجع سابق، ص 82.

(2) المصدر السابق، ص 79.

(3) يجب عدم الخلط بين برنامج الحاسوب وبين الوسيط المادي الذي افرغ عليه البرنامج (Material Object) وهو الوعاء الذي خزن أو حمل او ثبت فيه البرنامج أكان الوعاء قرصاً مرناً (Flopy Disk) ام قرصاً مضغوطاً C. D ام شريطاً ممغنطاً ام رقيقة أو شريحة Chip ، او ذاكرة الحاسوب أياً كان نوعها او أي وسيلة أخرى قد تخترع مستقبلاً. انظر، الحفناوي، مرجع سابق، ص 83.

(4) المصدر السابق، ص 79.

1- برمجيات النظم (Operating System or System Software):

وتقوم هذه البرمجيات بوظيفة إجرائية، حيث تسيطر على العمليات الأساسية للأداء الآلي داخل الحاسوب[1].

بعض هذه البرمجيات يبنى داخل جهاز الحاسوب وبعضها يخزن على الأقراص المغنطة ويجب شراؤه بشكل منفصل. ومن هذه البرمجيات لغات البرمجة[2] والمترجمات ونظم التشغيل.

2- البرمجيات التطبيقية (Applications Soft ware):

هي برامج مصممة ومنتجة لتؤدي وظائف معينة تستجيب لاحتياجات العملاء ومتطلباتهم، والبرامج التطبيقية لا تقع تحت حصر، ومن أمثلتها البرامج المستخدمة في البنوك والمؤسسات المالية لتؤدي وظائف معينة مثل: مسك حسابات العملاء أو الربط بين فروع البنك[3].

المطلب الثالث: التطور التاريخي لجهاز الحاسوب

17 ـ مرَ جهاز الحاسوب بعدة مراحل حتى وصل إلى هذه المرحلة المتقدمة والمتطورة حيث أصبحت المجتمعات تعتمد بصورة رئيسية في انجاز مهماتها وأداء نشاطاتها على وجوده.

والمراحل أو الأجيال الأساسية التي مرت بها الحواسيب يمكن تصنيفها كالآتي:

---

(1) الغريب، مرجع سابق، ص 35.

(2) البرمجة هي عملية كتابة أو وضع البرامج. ولغات البرمجة هي عبارة عن تدوين مجموعة خاصة من العلامات او الرموز يعبر بها عن البرنامج . فلغات البرمجة هي لغات مصطنعة ولذلك فليس هناك حرية في التعبير كتلك التي تتميز بها اللغات الإنسانية. وهناك العديد من لغات البرمجة المستخدمة، ويتم تصميم كل منها لحل نوع خاص من المشكلات ومن أهم لغات البرمجة المعروفة فورتران Fortran والكوبول Cobol والباسكال Pascal وسي C وجافا Java. انظر، الحفناوي، مرجع سابق، 97. الزعبي وآخرون، مرجع سابق، ص35.

(3) الحفناوي، مرجع سابق، ص 89.

الجيل الأول: (1951 - 1959)

في بداية عام 1951 تم تطوير أول جهاز حاسوب للأغراض التجارية يدعى (Univarcal) على يد العالمان (Mauchly and Eckert).

ومن خصائص حواسيب هذا الجيل استخدام الصمامات المفرغة التي تتميز بأنها: غالية الثمن، وتولد حرارة عالية وبطيئة[1]. كما أن حجم حواسيب هذا الجيل كبير وعملية البرمجة صعبة حيث استخدمت في هذا الجيل لغة الآلة التي تعتبر صعبة ومعقدة مقارنة بلغات البرمجة التي ظهرت لاحقاً[2].

الجيل الثاني: (1959 - 1964)

وتميز هذا الجيل بظهور الترانزيستور[3] كاختراع جديد في عالم الالكترونيات الذي يمتلك مزايا عديدة لا يمتلكها الصمام المفرغ، حيث زادت سرعة تنفيذ العمليات الحسابية، وكان هناك انخفاض نسبي في الحجم والكلفة. كذلك تم استخدام لغات برمجة مثل لغة فورتران ولغة كوبول بدلاً من لغة الآلة.

كما أن هناك تطوراً مهماً في أجهزة الإدخال والإخراج حيث استعملت الأشرطة المغناطيسية كذاكرة مساعدة[4].

الجيل الثالث: (1964- 1970)

شهد هذا الجيل ولادة الدوائر المتكاملة التي كان لها اثر كبير في تصغير حجم الحواسيب، كما زادت سرعة العمليات وانخفضت تكاليف جهاز الحاسوب، كما تم

---

(1) الغريب، مرجع سابق، ص 12.

(2) القاضي، اساسيات علم الحاسوب... مرجع سابق، ص 11، 12.

(3) الترانزيستور عبارة عن قطعة معدنية صغيرة جداً على شكل حلقة ممغنطة استعملت لتخزين المعلومات. وقد قام ثلاثة علماء في مختبرات شركة الهاتف الأمريكية (بل) باختراع الترانزيستور وكانت الأخيرة تتألف من لفافة سيلكون وهي مادة شبه موصلة مصنوعة من الرمل وتتميز هذه المادة بأنها لا تدع التيار الكهربائي يمر عبرها بسهولة كما انها لا تمنعه من المرور، وهكذا أصبحت الحواسيب الترانزستورية أصغر من سابقتها واسرع واقوى. انظر، اتليسك، جين. كل شيء عن الحواسيب، (ترجمة مركز التعريب والترجمة) . ط1، الدار الجامعية للنشر، بيروت، 1994، ص7،6.

(4) القاضي، اساسيات علم الحاسوب... مرجع سابق، ص 12، 13.

تحسين أجهزة الإدخال والإخراج حيث أدخلت تعديلات على الأقراص المغناطيسية والشاشات[1].

الجيل الرابع: (1970 - 1981)

امتاز هذا الجيل بتطوير الدوائر المتكاملة، وازدادت سرعة العمليات بشكل اكبر. كما تم تطوير رقائق صغيرة جدا من السيلكون Silicon تدعى المعالج الميكروي، و في هذا الجيل تم إدخال تحسينات كبيرة على أجهزة الإدخال والإخراج.

الجيل الخامس: (1981 - 1991)

بدأ هذا الجيل بعقد مؤتمر دولي في طوكيو في العام1981 حيث أعلن اليابانيون[2] مشروع الجيل الخامس للحاسبات الالكترونية مع التطور الفائق للذكاء الصناعي وإنتاج حاسبات لها القدرة على الاستنتاج بصورة سريعة وسرعة تصل إلى (1000) مليون عملية في الثانية باستخدام وسائل المعالجات المختلفة[3].

إن أجهزة الجيل الخامس وبرمجياته لها وظائف متقدمة تتمثل في معالجة المعلومات والحقائق والمعارف باستخدام ميكانيكية الاستقراء (INFERENCE) التي

(1) القاضي، اساسيات علم الحاسب... مرجع سابق. ص 13.

(2) يشار إلى أن تطوير حاسبات الجيل الخامس في اليابان شملت ثلاثة مراحل:

المرحلة الأولى: امتدت من عام 1982 – 1984 وشملت هذه المرحلة تطوير تقنية الحاسوب من حيث القدرة والشكل وتطوير الأجزاء التقنية في لغات البرمجة التي تدعم وظيفة الاستقراء.

المرحلة الثانية: امتدت من عام 1985 – 1988 وتضمنت تطوير نموذج تجريبي صغير للمنظومة المرجوة وتقييم الجدوى والأداء بالإضافة إلى مزيد من البحث والتطوير في استخدام ميكانيكية قواعد المعرفة Knowledge base في هذه المنظومة.

المرحلة الثالثة: امتدت من عام 1989 – 1991 فكانت المرحلة النهائية في عملية تنفيذ نتائج البحث والتطوير لميكانيكية الاستقراء وتم بناء نموذج لحاسبات الجيل الخامس.انظر، البياتي، هلال. استخدام الحاسبات الفنية وحمايتها. ورقة عمل مقدمة إلى ندوة القانون و الحاسوب المنعقد في العراق (1998)، بيت الحكمة، بغداد، ص 34.

(3) الغريب، مرجع سابق، ص 13.

هي عبارة عن قواعد تستخدم المعرفة والحقائق لاستخلاص معلومات غير معروفة من معلومات معروفة[1].

الجيل السادس: (1992 – حتى الوقت الحاضر)

أطلق مشروع حواسيب الجيل السادس في شهر آذار 1992. ومن خصائصه تقليد الدماغ البشري والتشبه به، فهناك محاولات لتقريب الأسلوب المتبع في معالجة المعلومات مع الأسلوب البشري.

وتتركز تقنيات حواسيب الجيل السادس على مفاهيم الشبكات العصبية والمعالجات المتوازية[2].

(1) البياتي، مرجع سابق، ص 34.

(2) تقنيات الشبكات العصبية تشمل تصميم برامج خبيرة تحاكي الشبكة العصبية لدماغ الإنسان حيث تستطيع هذه الحاسبات التعامل مع المعلومات بسرعات تتعدى سرعات الحاسبات السابقة بآلاف المرات، ويمكنها تفسير الكلام البشري وتشخيص الأجسام والصور بالأبعاد الثلاثة، أي أن الشبكة العصبية مبنية على عدد من المعالجات المتداخلة والمترابطة مشابهة إلى الخلايا العصبية في الدماغ.

أما تقنيات المعالجة المتوازية فهي عنصر من العناصر المهمة الأخرى في حاسبات الجيل السادس، حيث أصبح بالإمكان معالجة(5) إلى (15) بليون عملية حسابية في الثانية، وذلك بوضع أكثر من (600) معالج دقيق تعمل بشكل متواز لمعالجة البيانات والإيعازات المطلوبة. انظر، البياتي، مرجع سابق، ص 34، 35.

المبحث الثاني
الجانب الفني والتقني لشبكة الإنترنت

18- حدث خلال القرن العشرين نمو نوعي لحجم ومقاييس المعلومات والمعارف المتداولة وسمي ذلك بالانفجار المعلوماتي أو الثورة المعلوماتية، وباتت صناعة المعلوماتية في العقود الأخيرة الموجه الرئيسي لتسريع التقدم العلمي[1].

وكان لظهور الإنترنت أثر كبير في انتقال المعلومات وتداولها والاستفادة منها في وقت قياسي في أي مكان في العالم. فالإنترنت ساهم بشكل لا نظير له في صناعة المعلومات وثورتها فهو أحد العناصر الرئيسة التي ترتكز عليها تكنولوجيا المعلومات[2].

وللوقوف على الجانب الفني والتقني لشبكة الانترنت سوف نتناول تعريفها وذلك في (المطلب الأول)، ثم نعرض للتطور التاريخي الذي مرت به هذه الشبكة في (المطلب الثاني)، وأخيراً نستعرض أهم الخدمات التي تقدمها شبكة الانترنت التي جعلت العالم قرية صغيرة في (المطلب الثالث).

المطلب الأول: تعريف الإنترنت (Internet)

19- الإنترنت كلمة انجليزية مركبة مختصرة مكونة من مقطعين (Inter) اختصارا للكلمة الانجليزية (International) وتعني دولي و(Net) اختصارا لكلمة (Network) وتعني شبكة. والإنترنت هي الشبكة العالمية للمعلومات.

والإنترنت أو الشبكة العالمية للمعلومات عبارة عن شبكة ضخمة من الحواسيب المتصلة فيما بينها حول العالم التي يتم من خلالها تبادل المعلومات. وقد تكون هذه

---

(1) النقري، معن. المعلوماتية والمجتمع ط1، المركز الثقافي العربي، الدار البيضاء، 2001، ص 14.

(2) تكنولوجيا المعلومات عبارة عن مجموعة الأدوات التي تساعد في استقبال المعلومة ومعالجتها وتخزينها واسترجاعها وطباعتها ونقلها بشكل الكتروني سواء اكانت على شكل نص او صوت او صورة او فيديو، وذلك باستخدام الحاسوب. ومن هذه الأدوات الحاسوب والطابعة والأقراص والانترنت وغيرها الكثير انظر، الزعبي وآخرون، مرجع سابق، ص 6.

الشبكات محلية (Local Area Network L A N)[1] تربط مجموعة حواسيب قريبة من بعضها البعض وتشترك في المعدات المادية وتشترك أيضا في البرامج والبيانات. فقد تجمع كل إدارة من إدارات مؤسسة أو شركة ضخمة حواسيبها في شبكة محلية وترتبط الحواسيب المحلية عن طريق حاسوب واحد على الأقل يمتاز بالسرعة العالية وقدرة تخزين كبيرة[2].

20 ـ وهناك الشبكات الموسعة أو العامة (Wide Area Net work WAN) وهذه الشبكات الموسعة تربط طرفيات حواسيب منتشرة في مناطق جغرافية واسعة كالمدن والدول وحتى القارات.

وترتبط هذه الحواسيب مع بعضها عن طريق قنوات اتصال مثل خطوط التلفون والميكرويف والأقمار الصناعية، ويطلق على الشبكات الموسعة اسم شبكات نقل البيانات العمومية (Public Data Net works)[3].

فالإنترنت عبارة عن أكبر شبكة حواسيب[4] موسعة تغطي جميع أنحاء العالم، تصل بين حواسيب شخصية، وشبكات محلية، وشبكات عامة. ويمكن لأي شخص

---

(1) والشبكة المحلية L A N نوعان:

1- شبكة الخادم والعملاء (Clint Server Architecture) وهذه الشبكة تتميز بوجود حاسوب يسمى (Server) يقدم الخدمات من الشبكة إلى حواسيب اخرى تسمى عملاء (Clients) ترتبط معه.

2- شبكة نظير لنظير (Peer – To – Peer Architecture) وفي هذه الشبكة كل الأجهزة متساوية ومتكافئة وبإمكان اي جهاز في الشبكة أن يكون خادماً أو عميلاً في الوقت نفسه، اي انه لا يوجد جهاز مميز عن الأجهزة الأخرى، وهذه أقل كلفة من الشبكة التي سبقتها، وتستخدم في المنشآت ذات الأعمال البسيطة. الزعبي وآخرون، مرجع سابق، ص 46.

(2) القاضي، زياد، و القاضي، قصي واللحام، علي، ومحمود، سالم، ومجدلاوي، يوسف. مقدمة إلى الإنترنت، ط1، دار صفاء للنشر والتوزيع، عمان، 2000، ص 17.

(3) الزعبي وآخرون، مرجع سابق، ص 47. انظر كذلك في تعريف الإنترنت، الصمادي، حازم. المسؤولية في العمليات المصرفية الإلكترونية، ط1، دار وائل للنشر، عمان، 2003، ص27.

(4) تعرف شبكة الحواسيب (Computer Net work) على أنها مجموعة حواسيب مرتبطة معاً (عن طريق الكوابل او خطوط التلفون أو خطوط نقل البيانات السريعة أو الأقمار الصناعية) بحيث تشترك هذه الحواسيب في المصادر نفسها المادية والمعلومات. انظر، القاضي وآخرون، مقدمة إلى الانترنت... مرجع سابق، ص 17.

أن يصبح عضواً في هذه الشبكة من منزله أو مكتبه أو أي مكان آخر، ويستطيع حينها الوصول إلى قدر هائل من المعلومات عن أي موضوع[1].

21 ـ إن تواصل المستخدم مع الشبكة العالمية للمعلومات (الإنترنت) يتطلب توافر جهاز حاسوب وتقنية تدعى مودم[2]، وخط هاتف، وكذلك برمجيات الإنترنت وتسمى المتصفحات، وعادة تأتي مع نظام التشغيل عند الحصول على الحاسوب. وبتوافر هذه المتطلبات الأساسية يستطيع المشترك الاستفادة من الخدمات التي تقدمها الشبكة.

22 ـ والإنترنت لا يملكها احد ولا يسيطر عليها احد، إنما هي ملكية تعاونية للبشرية جميعها بقدر إسهامهم فيها، فلا توجد إدارة مركزية للإنترنت.

وقد وصفها البعض بأنها فوضى تعاونية؛ ذلك بأن كل شبكة مشتركة في الإنترنت لها قواعدها الخاصة والهيكل التنظيمي لإدارتها. ولكن هذه الشبكات لا يمكن الاتصال بينها إلا إذا كان هناك تعاون بينهما؛ ولذلك هناك الكثير من اللجان ومجموعات العمل التي تمثل فيها كل شركات المعلومات هي في اجتماعات مستمرة من اجل الوصول إلى وضع الأسس والضمانات التي تكفل تحسين الأداء في الشبكة العالمية وتطوير أسلوب التشغيل والاتفاق على المصطلحات والمستجدات التكنولوجية التي تطرأ من حين لآخر[3].

فلا يمكن القول حاليا: إن هناك أحداً يملك الإنترنت، ففي البداية كانت وزارة الدفاع الأمريكية ثم المؤسسة القومية للعلوم الأمريكية هي المالك الوحيد للشبكة. ولكن بعد تطور الشبكة ونموها اختفى مفهوم التملك ليحل محله ما أصبح يسمى

---

(1) الزعبي وآخرون، مرجع سابق، ص50.

(2) المودم Modem عبارة عن وحدة ربط تستخدم في إرسال واستقبال البيانات عبر خطوط الهاتف وبما أن الحواسيب تتعامل مع الإشارات الرقمية (Digital singals) بينما صممت خطوط الهاتف لتحمل الإشارات التناظرية (Analog Singals) وهي اصوات المستخدمين، فإن وظيفة المودم تحويل الإشارات العددية إلى إشارات تناظرية لنقلها عبر خطوط الهاتف. ابرز المصطلحات التقنية المستخدمة في الانترنت، مجلة الكمبيوتر والاتصالات والالكترونيات، المجلد(12) العدد(7)، ايلول 1995، ص 73.

(3) حجازي، عبد الفتاح بيومي. الاحداث والانترنت، ط1، دار الفكر الجامعي، الاسكندرية، 2002، ص 20، 21.

بمجتمع الإنترنت الافتراضي[1] كما أن تمويل الشبكة تحول من القطاع الحكومي إلى القطاع الخاص.

المطلب الثاني: التطور التاريخي لشبكة الإنترنت

23 ـ بداية الإنترنت تعود إلى العام 1969، عندما أنشأت وزارة الدفاع الأمريكية وكالة مشاريع الأبحاث المتقدمة (Advanced Research Projects Admin (ARPA .

حيث وجدت وزارة الدفاع أنها بحاجة إلى شبكة اتصالات يمكن أن تصمد أثناء الحرب، وكان الهدف منها تصميم شبكة إذا دمر قسم منها بسلاح نووي، يمكن أن ترسل مع ذلك رسالة تجد طريقها إلى مقصدها، وكانت النتيجة شبكة (ARPA NET)[2].

أي أن بداية ظهور شبكة الانترنت كانت لتحقيق أغراض عسكرية، حيث كانت تربط بين مراكز الحواسيب المختلفة وأنظمة الراديو والأقمار الصناعية الخاصة بالولايات المتحدة الأمريكية في كل أنحاء العالم.

24 ـ وبعد ذلك تطور المشروع وتحول إلى الاستعمال السلمي، فمع حلول عام 1983 استخدمت (ARPANET) بكثافة كبيرة وخصوصاً من قبل الجامعات إلى حد أنها بدأت تعاني من ازدحام يفوق طاقتها وصار من الضروري إنشاء شبكة جديدة فظهرت شبكة (MILNET) لتخدم المواقع العسكرية فقط.

وشبكة (ARPANET) بقيت لتتولى أمر الاتصالات غير العسكرية مع بقائها موصولة بشبكة (MILNET) من خلال برنامج اسمه بروتوكول (IP)[3].

وفي عام 1984 أصبحت إدارة (ARPANT) من مسؤولية مؤسسة العلوم الوطنية الأمريكية (NSF)، حيث قامت هذه المؤسسة بشراء حواسيب عملاقة (Super Computer)

---

(1) مجتمع الانترنت أصبح يشكل الآن حسبما يرى البعض دولة جديدة هي دولة المتعاملين مع الانترنت، وسيبلغ تعداد سكانها أكثر من حوالي 40 مليون مواطن يتزايدون بنسبة 5٪ شهرياً. أنظر، رمضان، مدحت. جرائم الاعتداء على الأشخاص والانترنت، ط1، دار النهضة العربية، القاهرة، 2000، ص 5.

(2) هونيكوت، جيري. مبادئ الإنترنت (ترجمة عمر الأيوبي)، ط1، أكاديميا، بيروت، ص 18.

(3) البياتي، مرجع سابق، ص 24، 25.

وتزويد مراكز الحاسوب بها، ثم توزيعها على كل مناطق الولايات المتحدة الأمريكية حتى تعمل مع بعضها البعض في شكل شبكة قومية.

وكانت شبكة الإنترنت في هذه المرحلة ما زالت مخصصة لأغراض البحث العلمي وتيسر للعلماء الاستفادة من إمكاناتها الهائلة في القيام بالعمليات الرياضية المعقدة[1] وغيرها من الأمور.

25 ـ مع حلول عام 1990 عانت شبكة (ARPANET) من البطء وظهر فيها الكثير من العيوب، كما إن ظهور حواسيب أصغر حجماً وأكثر قوة من الحواسيب المتوسطة أدى إلى ضعف شبكة (NSFNET).

إن الحاجة الماسة إلى استخدام الشبكات نفسها لأغراض تجارية يستفيد منها الأفراد والشركات والمؤسسات أدى إلى تطور الشبكة من الجانب التجاري حيث ابتدع عدد من الشركات الكبرى شبكاتهم العالمية. أضف إلى ذلك أن الإصدار الأول من موزاييك (MOSAIC) مستعرض الشبكة العالمية عام 1993 وما تبعه من إصدار (نتسكيب) و(مايكروسوفت)[2]. كل هذه الأمور أدت إلى تطور شبكة الإنترنت بالصورة التي نراها عليها الآن، حيث تربط هذه الشبكة في الوقت الحاضر بين ملايين الحواسيب الممتدة عبر قارات العالم، وهناك ملايين المشتركين والمستخدمين الذين يستعملون هذه الشبكة لأغراض مختلفة لتحقيق أهداف تتنوع حسب مراكز هؤلاء الأشخاص وطبيعة أعمالهم.

المطلب الثالث: خدمات الإنترنت

26 ـ مجتمع الإنترنت الرحب فتح الباب واسعاً أمام التدفق الهائل للمعلومات التي تنساب من قارة إلى أخرى في زمن قياسي الأمر الذي وفر على المستخدم الجهد والوقت الذي كان سيبذله في حال عدم وجود هذه الشبكة.

---

(1) حجازي، الأحداث والإنترنت... مرجع سابق، ص 18، 19.

(2) البياتي، مرجع سابق، ص 25، 26.

إن سهولة استخدام شبكة الانترنت والخدمات المتعددة والمتنوعة التي تقدمها في جميع مجالات الحياة ساهم بشكل فعال في زيادة أعداد المستفيدين منها. وسنقوم باستعراض أهم الخدمات الالكترونية التي تقدمها الشبكة العالمية للمعلومات "الإنترنت":

أولا: البريد الالكتروني (MAIL – E)

27 ـ يعتبر البريد الالكتروني[1] من الاستخدامات الشائعة التي توفر إمكانية الاتصال بملايين البشر حول العالم كبديل للبريد التقليدي. والبريد الالكتروني عبارة عن: رسالة لكنها تتم بطريقة الكترونية يكتبها المستخدم على جهاز الحاسوب، و ذلك بعد أن يفتح الصفحة الخاصة ببريده الالكتروني التي لها رقم سري واسم للمستخدم ولا يمكن لغيره الدخول إليها، وبعد إتمام كتابة الرسالة يقوم المستخدم بالضغط على أمر معين في الصفحة وهو (SEND) أي أرسل وفي حال تمام إرسال الرسالة يظهر على جهاز الحاسوب ما يفيد تمام العملية بنجاح، وإذا كان هناك خطأ ما يظهر للمرسل رسالة موجزة تشير إلى موضع الخطأ[2].

28 ـ يتيح البريد الالكتروني إمكانية نقل الرسائل بطريقة سريعة للغاية وكلفة المكالمة الهاتفية المحلية. وتتوافر في البريد الالكتروني عوامل الأمان والسرية؛ فلا يمكن اختراق البريد الالكتروني لشخص إلا بمعرفة كلمة السر الخاصة به أو من خلال طرق فنية معقدة لا يجيدها إلا محترفي عمليات اختراق شبكات الحاسوب[3].

---

(1) تجدر الإشارة إلى أن قانون المعاملات الإلكترونية المؤقت رقم (85) لسنة (2001) عرف كلمة الإلكتروني على أنها، (تقنية استخدام وسائل كهربائية أو مغناطيسية أو أي وسائل مشابهة في تبادل المعلومات وتخزينها) . كما يعرف ذات القانون كلمة الإلكترونية على أنها، (معالجة المعلومات).

(2) حجازي، الأحداث والانترنت... مرجع سابق، ص 23.

(3) خدمة أخرى تلحق بالبريد الإلكتروني على الإنترنت تسمى القوائم البريدية، ويقصد بالقائمة البريدية " نظام إدارة وتصميم الرسائل والوثائق على مجموعة من الأشخاص المشتركين في القائمة ـ عبر البريد الإلكتروني ـ وتغطي القوائم مواضيع ومجالات شتى وتتناول كل قائمة عادة موضوعاً محددا. وحتى يمكن لمستخدم الإنترنت الاشتراك في إحدى قوائم البريد الإلكتروني فلا بد أن يكون له صفحة وموقع في البريد الإلكتروني حتى تتم مراسلته على ذلك العنوان. انظر، حجازي، الاحداث والانترنت... مرجع سابق، ص 23، 24.

ثانياً: شبكة العنكبوت العملاقة (World Wide Web)

29 ـ المعروفة بـ (WWW) التي تتيح للمستخدم تصفح مواقع (Sites) المعلومات وهذه الخدمة تجمع النصوص والصور والأصوات والأفلام المتحركة، مما يتيح للمستخدم الحصول على المعلومات التي يريدها في أسرع وقت.

ثالثاً: محركات البحث (Search Engines)

30 ـ هي عبارة عن برامج تساعد في الحصول على المعلومات، فكما هو معروف هناك كم هائل من المعلومات في شبكة الإنترنت يرغب المستخدم في معرفة المواقع التي تمكنه من الوصول مباشرة إلى مبتغاه، فيتم في هذه الحالة إخبار خدمة البحث باسم الموضوع الذي يهم المستخدم و من ثم يتم تزويده بقائمة المواقع التي تتطابق مع المعلومات التي يرغب في الحصول عليها. وهناك عدة محركات بحث كل منها يستخدم طريقة معينة أو خاصة في إجراء عملية البحث[1].

رابعاً: التخاطب عبر الانترنت (Chat)

31 ـ يقوم المستخدم في عملية التخاطب بكتابة رسالة يجري عرضها مباشرة أمام شخص آخر في أي مكان في العالم الذي يقوم بدوره بالرد مباشرة على هذه الرسالة.

يشغل التخاطب عبر الانترنت مساحة كبيرة من حزمة البيانات التي يتم تبادلها بين مستخدمي هذه الشبكة العالمية، وبالرغم من أن التخاطب وسيلة اتصال إلا أنها الدافع الرئيسي لأكثر من 25% من المستخدمين لهذه الشبكة. ومن مزايا التخاطب عبر شبكة الانترنت: أنه نوع من الحوار الفكري الذي إذا تم بالشكل والأسلوب الصحيحين فإنه سيؤدي إلى التبادل الثقافي بين الحضارات.

---

(1) من محركات البحث المشهورة Yahoo وgoggle ، ومن اهم عناصر برامج البحث هو العنكبوت السوبر Super Spider وهو عميل صغير يتجول في الإنترنت باحثاً عن المعلومات في مواقع الشبكة العالمية. انظر، البياتي، مرجع سابق، ص 31،30.

وكذلك، الزعبي وآخرون، مرجع سابق، ص 51.

خامساً: المجموعات الإخبارية (News groups)

32 ـ مجموعات الأخبار عبارة عن أماكن وساحات افتراضية للقاء و التحادث بين مستخدمي شبكة الإنترنت من ذوي الاهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل للبيانات والمعلومات والأفكار حول موضوع معين.

سادساً: التجارة الالكترونية

33ـ يعكس مدلول التجارة الالكترونية استخدام التقنيات الحديثة في المعلومات والاتصالات من أجل إبرام الصفقات وعقد المبادلات التجارية[1].

34ـ وقد أتاحت شبكة الإنترنت لطرفي العقد التقابل وجها لوجه بالصوت والصورة رغم تباعدهما آلاف الأميال والاتفاق على التفصيلات الدقيقة بعد إبداء الإيجاب، ثم القبول بطريق الإنترنت، ثم إبرام العقد والتوقيع عليه بطريق التوقيع الالكتروني[2] دون حاجة لاجتماع المتعاقدين في مكان واحد. وإبرام العقد يتم بعد أن يكون البائع أو المورد أو مقدم الخدمة قد أعلن عنها بصورة واضحة وكافية على شبكة الإنترنت، حيث يكون الطرف الآخر قد اطّلع على هذا الإعلان وحصل على الإيضاحات والتفسيرات المطلوبة بشأن السلعة.

ويمكن للمشتري أو المستورد أن يسدد قيمة بضاعته عن طريق الدفع بواسطة شبكة الانترنت، ويكفيه في ذلك رقم حسابه البنكي ورقم بطاقة الائتمان الخاصة به[3].

---

(1) الزيدي، وليد. القرصنة على الانترنت والحاسوب، ط 1، دار أسامه للنشر، عمان، ص 59.

(2) عرف التوقيع الالكتروني في قانون المعاملات الالكترونية الأردني رقم 85 لسنة 2001 على انه، " البيانات التي تتخذ هيئة حروف أو ارقام او رموز أو إشارات أو غيرها وتكون مدرجة بشكل الكتروني او رقمي او ضوئي او اي وسيلة اخرى مماثلة في رسالة معلومات او مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من اجل توقيعه ويغرض الموافقة على مضمونه ".

(3) حجازي، الاحداث والانترنت... مرجع سابق، ص31 .

ونمو التجارة الالكترونية يرتبط بمدى التقدم التكنولوجي، ولذلك فالدول المتقدمة معلوماتياً تقوم غالباً بدور المنتج، في حين تبقى الدول الناشئة في دور المتلقي لهذه التقنيات إذ تكون غالباً في عداد المستهلكين في شأن التجارة الالكترونية[1].

سابعاً: بروتوكول نقل الملفات File Transfer Protocol (F T P)

35 ـ تمكن هذه الخدمة المستخدم من نسخ الملفات من جهاز حاسوب إلى جهاز آخر؛ وعليه يستطيع الباحثون الحصول على احدث الأبحاث العلمية من الجامعات ومراكز البحوث بسرعة كبيرة[2].

---

(1) حجازي، عبد الفتاح. النظام القانوني لحماية التجارة الالكترونية، (الكتاب الثاني)، ط1، دار الفكر الجامعي، الاسكندرية، 2002، ص 10.

(2) هناك خدمات أخرى يمكن لشبكة الانترنت أن تقدمها، منها:

- إمكانية تصميم المواقع (Sites) على شبكة الإنترنت، حيث يستطيع المستخدم تصميم الموقع الخاص به بهدف تحقيق غرض معين.
- النشر الالكتروني للصحف والمجلات والدوريات اليومية والشهرية، مما يتيح للقراء الإطلاع عليها دون الحاجة إلى شرائها، كما أن الانترنت وسيلة دعائية وإعلانية للعديد من السلع والبضائع.
- إتاحة الشبكة لبعض المرضى الحصول على الخدمات الطبية، وهذا ما يمكن التدليل عليه بقيام الحكومة البريطانية بإنشاء موقع يستطيع المرضى من خلاله الاتصال بالمرضين المدربين ووصف الأعراض المرضية التي تصيبهم. وهناك من يتحفظ على هذه الخدمة باعتبار انها قد تمد المريض بمعلومات خاطئة.

كما يمكن للجراحين الاستعانة بشبكة الانترنت عند إجراء العمليات الجراحية الدقيقة، وذلك عن طريق تصويرها بكاميرات فيديو لعرضها في مختلف انحاء العالم لأخذ رأيهم العلمي أثناء العملية الجراحية. انظر، حجازي، الاحداث والانترنت، مرجع سابق، ص 27، 28، 30. وكذلك، شلباية، مراد وفاروق، علي. مقدمة إلى الانترنت، ط1، دار المسيرة للنشر والتوزيع، عمان، 2001، ص 20، 21.

الفصل الأول
ماهية الجريمة المعلوماتية وسماتها العامة

الفصل الأول
ماهية الجريمة المعلوماتية وسماتها العامة

36 ـ الجريمة المعلوماتية: جريمة حديثة نسبياً، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنها اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم الأخرى، كما أن هذه الجريمة المعلوماتية جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

37 ـ وفي هذا الفصل سوف أتناول تعريف الجريمة المعلوماتية وأهم الخصائص التي تميزها عن غيرها من الأنماط الأخرى للجرائم.

ثم سأعرض لأهم الأسباب التي تستدعي الحماية الجنائية للمعلوماتية من الجرائم التي قد تقع عليها.

وأخيراً سأتناول دراسة المجرم المعلوماتي من حيث سماته وطوائفه ودوافعه.

المبحث الأول
ماهية الجريمة المعلوماتية وخصائصها

38 ـ عصر الإنترنت أو عصر السموات المفتوحة أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هذه الأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة[1].

ويبدو بالفعل أن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وأن المعلومات في حد ذاتها هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها[2].

وفي الواقع إن هذا الوجه المشرق لتقنية المعلومات يخلُ من الجانب المظلم الذي تمثل في الإجرام المعلوماتي والذي كان موجوداً ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب تتنوع وتتعدد.

المطلب الأول: تعريف الجريمة المعلوماتية

39 ـ بداية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها: فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية[3].

(1) احمد، هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2003، ص 12.

(2) هذا ما اشار له العالم الاجتماعي دانيل بل في كتابه قدوم مجتمع ما بعد الصناعي. مشار له عند، المصدر السابق، ص11.

(3) المعلوماتية هي كلمة مكونة من مقطعين، المقطع الأول Information والمقطع الثاني Automatique. ويرجع الفضل في اقتراح مصطلح المعلوماتية إلى الأستاذ Drefus حيث استخدمه عام 1962 لتمييز المعالجة الآلية للمعلومات وتبنته بعد ذلك الأكاديمية الفرنسية في ابريل 1966 ومنحته التعريف الآتي "علم المعالجة المنطقية للمعلومات التي=

وهناك جانب يرى أن هذه الجريمة ناشئة أساساً من التقدم التكنولوجي، ومدى التطور الذي يطرأ عليه، وهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات، ويفضل أن يطلق عليها اصطلاح "جرائم التكنولوجيا الحديثة" فهي جرائم تكنولوجيا باعتبارها مرتبطة ارتباطاً وثيقاً بالتكنولوجيا التي تعتمد أساسا على الحواسيب وغيرها من أجهزة تقنية قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظرا لحداثتها النسبية من ناحية وارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل[1].

ومن جانبنا فنحن نذهب مع الاتجاه الذي يفضل إطلاق اصطلاح الجريمة المعلوماتية على الجرائم المتعلقة بالحاسوب والإنترنت، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الإنترنت .

40 ـ التكنولوجيا الحديثة ـ كما نعلم ـ لا سيما تحديدا التكنولوجيا المتعلقة بتقنيات الحاسوب والإنترنت متطورة و متسارعة النمو، الأمر الذي يجعل من الصعب حصر صور الجرائم المعلوماتية وأنواعها.

وفي هذا الإطار آثر المشرع الانجليزي في قانون إساءة استخدام الحاسوب عام 1990 عدم وضع تعريف محدد لجرائم الحاسوب؛ بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة، تحسباً للتطور العلمي والتقني في المستقبل[2].

وتجدر الإشارة إلى أن المشرع الجزائي الأردني ـ كما هو معروف ـ لم يتطرق للجريمة المعلوماتية في قانون العقوبات المعمول به حاليا.

= تعتبر بمثابة دعامة للمعارف الانسانية والاتصالات في المجالات الفنية والاقتصادية والاجتماعية وذلك باستخدام معدات آلية " انظر، الشوا، سامي. ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، دار النهضة العربية، القاهرة، 1994، ص 4.

(1) عفيفي، عفيفي كامل. جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، بدون ناشر، 2000، ص20.

(2) المناعسة، اسامة والزعبي، جلال والهواوشة، صايل، جرائم الحاسب الآلي والانترنت، ط1، دار وائل للنشر، عمان، 2001، ص73.

41 - في إطار تعريف الفقه للجريمة المعلوماتية نجد أن الاتجاهات تباينت في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لمفهومها.

42 - فمن التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على أنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى"[1].

وحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

كذلك عرّفت الجريمة المعلوماتية أنها: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية"[2].

يرى الأستاذ (Tredmann) أن: "الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات".

ويرى الأستاذ (Mass) أن المقصود بالجريمة المعلوماتية: "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"[3].

كذلك عرفها الأستاذ (Rosenblatt) على أنها: "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه"[4].

كما نلاحظ فإن هذا التعريف يضيق من مفهوم الجريمة المعلوماتية، إذ يخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب أداة لارتكابها.

---

(1) قورة، نائلة، جرائم الحاسب الاقتصادية، ط1، دار النهضة العربية، القاهرة، 2004، 2003، ص21.

(2) مشار إلى هذا التعريف عند، أحمد، هلالي عبد اللاه، التزام الشاهد بالاعلام في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 1997، ص13.

(3) ورد عند المصدر السابق، ص6.

(4) مشار له عند، يونس، عرب، دليل امن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والانترنت، ط1، اتحاد المصارف العربية، 2002، ص213.

43 ـ في المقابل فإن هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية، فعرّفها البعض أنها: "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية"(1).

وتم تعريفها كذلك أنها "كل سلوك سلبيّ أم ايجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت"(2).

وقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 إلى تعريف الجريمة المعلوماتية أنها: "كلّ سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"(3).

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها "تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها؛ وتبعاً لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر"(4).

ويتبنى الخبير الأمريكي (Parker) مفهوماً واسعاً للجريمة المعلوماتية(5) حيث يشير إلى أنها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل".

كذلك يعرف الأساتذة (Vivant و Lestanc) الجريمة المعلوماتية أنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب"(6).

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص7. و دسامي الشوا ـ في مؤلفه المشار اليه سابقا ـ يفضل استخدام مصطلح الغش المعلوماتي على هذا النوع من الجرائم.

(2) الهيتي، محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004، ص152.

(3) مشار لهذا التعريف عند، قورة، مرجع سابق، ص23.

(4) مشار له عند، السعيد، كامل، "جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات"، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 324، 325.

(5) مشار له عند، الشوا، ثورة المعلومات... مرجع سابق، ص6.

(6) مشار له عند، المصدر السابق، ص6.

كما عرفت هذه الجريمة على أنها، "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الحاسوب"[(1)].

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنى التعريف الآتي للجريمة المعلوماتية[(2)] إنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".

ونحن من جانبنا نتفق مع هذا التعريف، إذ إنه تعريف حاول الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية سواء التي قد تقع بواسطة النظام المعلوماتي أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة الكترونية. فهذا التعريف لم يركز على فاعل الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل إنه حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.

المطلب الثاني: خصائص الجريمة المعلوماتية

44 ـ ارتباط الجريمة المعلوماتية بجهاز الحاسوب و شبكة الإنترنت أضفى عليها مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية هي:

أولا: الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول

45 ـ المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.

---

(1) مشار إلى هذا التعريف عند، المرزوقي، محمود محمد. (2003). جرائم الحاسب الالي. المجلة العربية للفقه والقضاء، تصدر عن الامانة العامة لجامعة الدول العربية، العدد الثامن والعشرون، ص 53.

(2) مؤتمر الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، الذي عقد في فينا في الفترة الواقعة مابين 10 ـ17 نيسان لعام 2000، مشار له عند، المناعسة وآخرون، مرجع سابق، ص78.

فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد[1]. فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[2].

46 ـ هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

47 ـ كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز) من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية، وتتلخص وقائع هذه القضية التي حدثت عام 1989 في قيام احد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)؛ إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس؛ وفي الثالث من فبراير من عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات

(1) قورة، مرجع سابق، ص47. وهذا يعود إلى عالمية ظاهرة الانترنت حيث ان المعلومات التي تبثها طليقة من اي قيد جغرافي. انظر، حسين، محمد، المسؤولية القانونية في مجال شبكات الانترنت، ط1، دار النهضة العربية، القاهرة، 2002، ص8.

(2) د. Ulrich Sieber، جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي (ترجمة سامي الشوا)، دار النهضة العربية، القاهرة، 1993، ص 58.

المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث إن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية

الثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث(فيروس)[1].

48 ـ ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية ونظراً للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها؛ تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم[2]. والتعاون الدولي يتمثل في المعاهدات و الاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية و تقديمهم للقضاء العادل.

49 ـ تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة. بالإضافة إلى أن نقص الخبرة لدى الشرطة و جهات الادعاء و القضاء في هذا

---

(1) انظر، قورة، مرجع سابق، ص48.

(2) تجدر الإشارة في هذا المجال إلى مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاقبة المجرمين والذي عقد في هافانا عام 1990 وفي قراره المتعلق بالجرائم ذات الصلة بالحاسوب ناشد المؤتمر الدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الحاسوب والتي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر إذا دعت الضرورة في تحديث القوانين والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان ان الجزاءات والقوانين الراهنة بشأن سلطات التحقيق و قبول الأدلة في الإجراءات القضائية تنطبق على الجرائم المعلوماتية وإدخال تغييرات مناسبة عليها إذا دعت الضرورة، كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات بما في ذلك دخولها حسب الاقتضاء أطرافاً في المعاهدات المتعلقة بتسليم المجرمين و تبادل المساعدة في المسائل المرتبطة بالجرائم ذات الصلة بالحاسوب.انظر، محمود، مرجع سابق، ص 361، 362.

المجال لتمحيص عناصر الجريمة إن وجدت و جمع الأدلة عنها للإدانة فيها يشكل عائقاً كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم[1].

50 ـ وبالتالي من أجل التصدي للإجرام المعلوماتي لا بد أن تعمل الدول في اتجاهين:

الأول: داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم.

الثاني: دولي عن طريق عقد الاتفاقيات الدولية، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم[2].

ثانياً: صعوبة اكتشاف الجريمة المعلوماتية

51 ـ تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة[3].

(1) عوض محمد محي الدين مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 362،361.

(2) من صور التعاون الفعال في مجال مكافحة الجريمة المعلوماتية يمكن الإشارة إلى اتفاقية بودابست (Budapest) والتي حرص فيها مجلس أوروبا على التصدي للاستخدام غير المشروع للحواسيب و شبكات المعلومات وقد وقعت هذه الاتفاقية المتعلقة بالإجرام المعلوماتي في 23 نوفمبر (2001) إيمانا من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغييرات العميقة التي حدثت بسبب الرقمية. و تشير المذكرة التفسيرية لهذه الاتفاقية إلى أن "... سهولة الوصول إلى المعلومات في النظم المعلوماتية مع الإمكانيات اللامحدودة لتبادلها وإرسالها بصرف النظر عن المسافات الجغرافية أدى إلى نمو هائل في حجم المعلومات المتاحة التي يمكن الحصول عليها بسهولة. و من خلال الاتصال بخدمات الاتصالات و المعلومات يستطيع المستخدمون اصطناع فضاء جديد يسمى الفضاء المعلوماتي (Cyber Space) الذي يستعمل أساساً لأغراض شرعية ولكن يمكن أن يخضع لسوء الاستخدام، إذ أن هناك احتمالاً لاستخدام شبكات الحاسوب والمعلومات الالكترونية في ارتكاب أعمال إجرامية. وعلى ذلك يجب على القانون الجنائي أن يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصاً واسعةً لإساءة استخدام إمكانيات الفضاء المعلوماتي وأن يعمل على ردع هذه الأفعال الإجرامية مع تطبيق السلطات القسرية المقررة في بيئة تكنولوجيا المعلومات". انظر، احمد ـ الجوانب الموضوعية والإجرائية لجرائم المعلوماتية... مرجع سابق، ص29 ـ 32.

(3) الصغير، جميل عبد الباقي، القانون الجنائي و التكنولوجيا الحديثة، ط1، دار النهضة العربية، القاهرة، 1992، ص 17.

حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية.

52 ـ ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي اثر خارجي بصورة مرئية. كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول و قارات أخرى، إذ أن الجريمة المعلوماتية ـ كما سبق وأشرنا ـ جريمة عابرة للدول (دولية). وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة[1] يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم.

فالجرائم المعلوماتية في أكثر صورها خفية لا يلحظها المجني عليه أو لا يدري حتى بوقوعها و الإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمراً ليس عسيراً في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالباً لدى مرتكبها[2].

53 ـ كما أن المجني علية يلعب دوراً رئيسياً في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له و تكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهزّ الثقة في كفاءتها[3].

---

(1) المصدر السابق، ص 17.

(2) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، اسيوط، 1994، ص16.

(3) وتشير بعض التقديرات إلى أن ما يتراوح بين 20 و25٪ من جرائم الحاسبات لا يتم الإبلاغ عنها مطلقاً خشية الاساءة إلى السمعة و في دراسة ــ وصفت بأنها تثير الذهول ــ أجريت على الف شركة من الشركات المنتجة لجهاز (Fortune500) اظهرت نتائجها أن 2٪ فقط من كل جرائم الحاسب هي التي يتم الإبلاغ عنها للشرطة أو لمكتب التحقيقات الفيدرالي. انظر، رستم، الجوانب الاجرائية... مرجع سابق، ص 25 – 26.

ويرى البعض أن للمجني عليه دوراً مثيراً للريبة في بعض الأحيان، فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل تعرضه للجريمة المعلوماتية أمراً مرتفعاً بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي، ويترتب على ذلك نتيجة أخرى تميز الجريمة المعلوماتية هي أن هناك إمكانية للحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم، إذ يعتمد ذلك أساساً على تطوير نظم الأمن الخاصة بأنظمة الحاسبات و شبكاتها[1].

54 - وفي الواقع فإن إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية يبدو أكثر وضوحاً في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها. حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلباً في السياسة التي يمكن أن توضع لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي[2].

وإلى جانب ذلك فإن المجني علية يتردد أحيانا في الإبلاغ عن هذه الجرائم خوفاً من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى

(1) قورة، مرجع سابق، ص46.

(2) من الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم الحاسبات التزاماً على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال، مع تقرير جزاء على الإخلال بهذا الالتزام. وعرض ذات الاقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضاً باعتبار انه ليس مقبولاً تحويل المجني عليه إلى مرتكب الجريمة. انظر، رستم. الجوانب الإجرائية... مرجع سابق، ص 25-27.

الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه[1].

ثالثاً: صعوبة إثبات الجريمة المعلوماتية

55 ـ اكتشاف الجريمة المعلوماتية أمر ـ كما سبق و اشرنا ـ ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب.

56 ـ فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق و الملاحقة. ففي هذه البيئة تكون البيانات و المعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل و محوه كلياً من قبل الفاعل أمراً في غاية السهولة.

ففي إحدى الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا تم اختراقه من قبل الغير[2].

57 ـ وتجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الاحداث، حيث تخلف آثاراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة

---

(1) الهيتي، مرجع سابق، ص 166.

(2) انظر، رستم، الجوانب الاجرائية... مرجع سابق، ص23.

مسرح الجريمة في الجريمة المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة و ذلك لسببين[1]:

الأول: إن الجريمة المعلوماتية لا تخلف آثاراً مادية.

الثاني: إن كثيراً من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبياً، الأمر الذي يعطي مجالا للجاني أو للآخرين أن يغيروا أو يتلفوا و يعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية.

58 ـ بالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء يشكل عائقاً أساسياً أمام إثبات الجريمة المعلوماتية ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت. ونتيجة لنقص الخبرة والتدريب كثيراً ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية فلا تبذل لكشف غموضها وضبط مرتكبيها جهوداً تتناسب وهذه الأهمية. بل إن المحقق قد يدمر الدليل بمحوه محتويات الاسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة[2].

رابعاً: أسلوب ارتكاب الجريمة المعلوماتية

59 ـ ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها. فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي الذي قد

(1) المعاينة يقصد بها إثبات حالة الأماكن والأشخاص والأشياء وكل ما يعتبر في كشف الحقيقة و المعاينة بهذا المعنى يستلزم الانتقال إلى محل الواقعة أو اي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة. انظر، حجازي، عبد الفتاح بيومي. الدليل الجنائي والتزوير في جرائم الكمبيوتر و الانترنت، ط1، دار الكتب القانونية، القاهرة، 2002، ص59.

(2) حجازي، الدليل الجنائي ... مرجع سابق، ص 28و29. انظر كذلك، القبائلي، سعد حماد، ضوابط الحماية الإجرائية لبرامج الحاسب الآلي، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، اربد، من 26ـ27ـ 4(2004)، ص 24

يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة..... فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (soft crime) لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين كل ذلك دون حاجة لسفك الدماء.

خامساً: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

60 ـ تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها. وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، و شخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب و تحويل المكاسب إليه[1].

61 ـ والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكاً سلبياً وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكاً ايجابياً وهو غالباً كذلك يتمثل في مساعدة فنية أو مادية[2].

سادساً: خصوصية مجرمي المعلوماتية

62 ـ المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي).

(1) عفيفي، مرجع سابق، ص 32

(2) الشوا، ثورة المعلومات وانعكاساتها.... مرجع سابق، ص46.

فإذا كانت الجرائم التقليدية لا اثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها - باعتبارها قاعدة عامة - فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.

فعلى سبيل المثال فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جداً من قبل مرتكبها.

كذلك فإن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.

وسوف نتناول موضوع المجرم المعلوماتي: سماته ودوافعه وطوائفه - بإذن الله - في مبحث مستقل ولذلك نحيل القارئ الكريم إليه منعاً للتكرار.

المبحث الثاني
دواعي الحماية الجنائية للمعلوماتية من الجرائم التي قد تقع عليها

63 ـ هناك أسباب عديدة تجعل الحاجة ملحة لحماية المعلوماتية من الجرائم التي قد تقع عليها. وتتمثل أهم هذه الأسباب في توجه الأردن نحو تطبيق شامل للحكومة الالكترونية في السنوات المقبلة، وكذلك الخسائر الفادحة التي قد تلحقها هذه الجرائم بالاقتصاد الوطني، وأخيراً عدم كفاية التشريعات الجنائية القائمة لمواجهة الاعتداءات التي قد تصيب المعلوماتية.

المطلب الأول: التوجه نحو الحكومة الالكترونية في الأردن

64 ـ كثر الحديث عن الحكومة الالكترونية في الفترة الأخيرة في ظل توجه عدد من الدول العربية نحو تنفيذ هذا المشروع الرائد الذي قد يكون الوسيلة الأفضل للتخلص من البيروقراطية والإجراءات الروتينية. وقد كانت مصر والإمارات العربية المتحدة والأردن من أوائل الدول التي بعثت الشرارة الأولى في سبيل إنشاء حكومة الكترونية تعتمد على التقنيات المعلوماتية.

والتوجه نحو إقامة حكومة الكترونية كأحد أهم الأسباب التي توجب الحماية الجنائية للمعلوماتية وتستدعيها تتطلب الحديث عن ماهية الحكومة الالكترونية وأهدافها ومراحل تطبيقها ومتطلبات قيامها ونجاحها.

أولاً: ماهية الحكومة الالكترونية وأهدافها (Electronic government)

65 ـ ظهور شبكة الإنترنت بخدماتها المتعددة كان له دوراً بارزاً في أن توجه كثير من الدول طاقاتها وإمكاناتها للاستفادة من هذه الشبكة، وكانت فكرة

الحكومة الالكترونية هي الثمرة التي خرجت بها بعض الدول[1] باعتبارها وسيلة لتسهيل معاملاتها الحكومية و الارتقاء بمستوى المواطن وتخفيف العبء على المؤسسات الحكومية المختلفة مما يؤدي إلى زيادة كفائتها.

66 ـ هناك عدد من التعريفات لمفهوم الحكومة الالكترونية منها: ما وضعته بعض المنظمات الدولية مثل البنك الدولي والأمم المتحدة ومنها التعريفات التي أخذت بها بعض دول العالم التي بدأت بتطبيق هذه التقنيات المعلوماتية التي تأخذ في الاعتبار الظروف الاقتصادية والاجتماعية ومراحل التقدم والتطور الذي حققته. ويمكن تعريف الحكومة الالكترونية أنها: (تحول الإجراءات الحكومية الداخلية أو الخارجية والمتمركزة حول توفير أو إيصال الخدمات للمتعاملين معها بفاعلية وكفاءة بصورة أفضل من خلال تقنيات المعلومات والاتصالات الحديثة) [2].

قيل أيضا في تعريف الحكومة الالكترونية أنها: "البيئة التي تتحقق فيها خدمات المواطنين واستعلاماتهم وتحقق فيها الأنشطة الحكومية للدائرة المعنية من دوائر الحكومة بذاتها أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات والاتصال عن بعد"[3].

وبناء عليه فان فكرة الحكومة الالكترونية تقوم على عدة ركائز هي تجميع الأنشطة والخدمات المعلوماتية والتفاعلية والتبادلية كلّها في موقع الحكومة الرسمي على شبكة الإنترنت في نشاط أشبه ما يكون بفكرة مجمعات الدوائر الحكومية،

(1) فكرة الحكومة الإلكترونية فكرة أثارها ونادى بها نائب الرئيس الأمريكي السابق آل جور ضمن تصور لدية لربط المواطن بمختلف أجهزة الحكومة للحصول على الخدمات الحكومية بأنواعها بشكل آلي مؤتمت إضافة إلى انجاز الحكومة ذاتها مختلف أنشطتها باعتماد شبكات الاتصال و المعلومات لخفض الكلفة و تحسين الأداء وسرعة الإنجاز وفعالية التنفيذ. مشار إلى ذلك عند، عرب، يونس، قانون الكمبيوتر، ط1، منشورات اتحاد المصارف العربية، 2001، ص445.

(2) مستقبل صناعة تقنية المعلومات في دول مجلس التعاون الخليجي، ورقة عمل قدمتها الأمانة الفنية لتقنية المعلومات بوزارة الاقتصاد الوطني في سلطنة عمان لمؤتمر الصناعيين التاسع لدول مجلس التعاون الخليجي، 2003، مجلة الغرفة، العدد (43)، ص (18).

(3) عرب، قانون الكمبيوتر... مرجع سابق، ص447.

وبعد ذلك تحقيق حالة اتصال دائم بالجمهور مع القدرة على تأمين الاحتياجات الاستعلامية والخدمية كلّها للمواطن[1].

67 ـ مشروع الحكومة الالكترونية يسعى إلى زيادة الإنتاجية والتنافسية وتسهيل التعامل بين الحكومة ومؤسساتها، كذلك بين الحكومة وقطاع الأعمال والمواطنين، حيث تتجسد الرؤيا في هذا المجال بانجاز المعاملات بيسر وسهولة بأدنى كلفة على المواطنين وقطاع الأعمال وذلك باستخدام الإنترنت[2].

كما يتم تقديم خدمات الكترونيا في مجال الرعاية الصحية وشؤون الهجرة والضرائب وفي مجال الاستثمار، تتم عملية الدفع أو السداد بطريقة الكترونية للجهات المختلفة. كما أنه في التصور الشامل للحكومة الالكترونية يمكن إنزال أي نموذج ورقي حكومي بصورة رقمية على الموقع الحكومي في شبكة الإنترنت وتعبئته وإعادة إرساله[3].

---

(1) انظر المصدر السابق، ص447. وتجدر الإشارة إلى أن الأردن قام بإنشاء موقع للحكومة الأردنية الالكترونية على شبكة الإنترنت لتحقيق الأغراض المنشودة من هذا المشروع الطموح وعنوان الموقع هو www.pm.gov.jo.

(2) العزام، احمد حسين. (2001). الحكومة الالكترونية في الأردن: إمكانيات التطبيق. رسالة ماجستير، جامعة اليرموك، اربد، الاردن. ص2.

(3) تجربة إمارة دبي هي تجربة رائدة في مجال تطبيق الحكومة الالكترونية فهذه الحكومة بدات عملها في تشرين الأول 2001 وذلك بتقديم أربع عشرة خدمة فقط ثم ارتفعت هذه الخدمات إلى 200 خدمة عام 2002 وإلى اكثر من 600 خدمة في عام 2003. وهذه الخدمات تقدم من خلال 19 دائرة حكومية مختلفة عبر بوابة الحكومة الالكترونية ويتوقع أن يتم توفير 70٪ من الخدمات الحكومية بصورة الكترونية بحلول العام 2005 و من الخدمات الجديدة التي استحدثتها الحكومة خدمة (Mdubai) التي تعتبر قناة تواصل الكترونية تسمح للدوائر الحكومية بالمشاركة في إرسال معلومات أو تنبيهات خاصة إلى الجمهور أو موظفيها عبر أجهزة المساعد الشخصي(ppa) او أجهزة الهواتف المتحركة. ومن الخدمات أيضاً المكتبة الالكترونية التي تقوم على دمج مكتبات الدوائر كلّها من خلال بوابة الكترونية واحدة حيث تكون المعلومات متاحة للجميع باقل قدر من الجهد وفي اسرع وقت ممكن. وتشمل الخدمات أيضاً التوظيف الالكتروني (EJOB) وهو عبارة عن منصة متطورة لمساعدة الباحثين عن فرص توظيف حيث يمكنهم تقديم بياناتهم و سيرتهم الذاتية و كذلك متابعة طلباتهم.

ومن الخدمات أيضاً خدمة اسأل دبي (ASK DUBAI) التي تتيح لقطاع رجال الأعمال إرسال استفساراتهم المتعلقة بالخدمات الحكومية عبر رقم هاتف مجاني موحد أو من خلال المحادثة المباشرة عبر الانترنت.

بالإضافة إلى ذلك تم توفير ما يزيد على 3000 برنامج تدريبي تفاعلي بالصوت والصورة وباللغتين الانجليزية والعربية لإفادة القطاع العام وشرائح المجتمع كلّه في التعرف على أساسيات التعامل مع الكمبيوتر والإنترنت وابجديات الوعي المعلوماتي.

انظر موقع WWW.ALJAZEERA.NETscience_ tech\2003\

68 ـ من أجل تحقيق هذه الأهداف جميعها قامت الحكومة الأردنية بتحديد أربعة محاور أساسية للعمل عليها بشكل متكامل ومتناسق.[1] وهذه المحاور هي التشريعات القانونية والتعليم والبنية التحتية و الخدمات الالكترونية. وما يهمنا في دراستنا هذه هو المحور الأول ألا وهو محور التشريعات القانونية.

ثانياً: مراحل الحكومة الالكترونية

69 ـ تجدر الإشارة إلى أن التطبيق الفوري للحكومة الالكترونية يتطلب موارد مالية كبيرة، وكذلك وجود موارد بشرية ذات تأهيل وتدريب عالي المستوى، وهما أمران لا يتوافران لمعظم البلدان وتحديدا بلدان المنطقة العربية.

70 ـ التدرج في أسلوب تنفيذ هذا المشروع الرائد هو وسيلة تضمن استمرارية الحكومة الالكترونية على أرض الواقع وتأديتها لوظائفها على أكمل وجه، كذلك يضمن أسلوب التدرج تقبل المواطنين لهذه الفكرة وتوعيتهم بمضمونها شيئا فشيئا. وأسلوب التنفيذ التدريجي هذا يمكن أن يتم وفق أربع مراحل:[2]

71 – المرحلة الأولى: التواجد

تقوم الحكومة في هذه المرحلة باستخدام الحكومة الالكترونية، لتوفير المعلومات والبيانات للمستخدمين من المواقع المختلفة للوزارات والوحدات الحكومية، دون الحاجة إلى الذهاب الفعلي لتلك الوزارات والوحدات، فعلى سبيل المثال: يستطيع المستثمر الحصول على المعلومات الخاصة بالضرائب من الموقع المختص أو الاطلاع على قوانين العمل وتعديلاتها...الخ.

---

(1) المدارس والمعاهد والجامعات الأردنية وكذلك القطاعات الأخرى كلها والمؤسسات تم تزويدها بآلاف الحواسيب ضمن خطة لشمول النظام التعليمي وغيره من القطاعات بثورة المعلومات، كما ينوي جلالة الملك عبد الله الثاني بن الحسين الإيعاز بتشييد منطقة صناعية خاصة بصناعات التقنية العالية وتكنولوجيا المعلومات حيث من المؤمل ان يستثمر المولون الأجانب ما قيمته 150 مليون دولار في السنوات الثلاث المقبلة.

انظر، الموقع الالكتروني:

WWW.NEWS.BBCCO.UK/HI/ARABIC/NEWS/NEWSID1640000/1640688.STM

(2) مجلة الغرفة، مرجع سابق، ص (19).

72 - المرحلة الثانية: التفاعل

وهي المرحلة التي تلي التواجد حيث يستطيع المواطن أو رجل الأعمال الاتصال المباشر عن طريق البريد الالكتروني مثلا بالمسؤول وتبادل الآراء والملاحظات حول القضايا المختلفة.

73 - المرحلة الثالثة: تنفيذ المعاملات الكترونياً

وهذه المرحلة من أكثر مراحل الحكومة الالكترونية تعقيداً، حيث إتمام المعاملات المختلفة مع الوحدات الحكومية مباشرة من خلال المواقع الالكترونية للحكومة ووحداتها، بما في ذلك السداد الالكتروني للرسوم والمدفوعات المتنوعة.

74 - المرحلة الرابعة: التحول النهائي

وهي آخر مراحل تنفيذ الحكومة الالكترونية حيث يصبح استخدام تقنية المعلومات والاتصالات في المعاملات كلّها ممارسة يومية عادية ومتوفرة في المناطق كلّها.

75 - بناء على استعراض هذه المراحل المختلفة للحكومة الالكترونية نستطيع القول بأننا في الأردن ما زلنا في المراحل الأولية وما زلنا نخط الخطى الأولى في تطبيق هذا المشروع الرائد.

وفي الواقع ان معظم تحديات الحكومة الالكترونية ومشاكلها قد تطفو على السطح في المرحلة الثالثة. و هذه التحديات تتطلب التدخل التشريعي الجنائي لحماية الأفراد وكذلك الحكومة من بعض الذين يستغلون هذه التقنيات الحديثة بما يحقق مصالحهم الشخصية ومطامعهم الاقتصادية.

ثالثاً: متطلبات الحكومة الإلكترونية

76 - إن السعي إلى استخدام تقنية المعلومات والاتصالات والتقدم العلمي في تقديم الخدمات وتوفير البيانات في القطاعين العام والخاص، وجعل الخدمة الآلية أو الالكترونية المحرك الأساسي لتوفير هذه الخدمات وتقديمها وإتاحتها للجميع لنقل الدولة إلى الحياة المبنية على المعرفة بشكل يخدم مختلف غايات التنمية وأغراضها

الشاملة، يتطلب وجود عدد من المعطيات أو العناصر التي دونها أو في حال تخلف احدها سيكون مشروع الحكومة الالكترونية عاجزاً عن تحقيق غاياته التي وضع ابتداء من أجلها، وأنفقت الدولة في سبيل إتمامه مبالغ كبيرة. والمعطيات المطلوبة لقيام الحكومة الالكترونية تشمل عدداً من الأمور أهمها:

77 – 1- المعطيات البشرية:

السعي لإقامة حكومة إلكترونية يستدعي العمل على تقليص الفجوة الرقمية لدى المواطنين؛ وذلك بمحو الأمية المعلوماتية لديهم وتوفير الكفاءات القادرة على التعامل مع أنظمة المعلومات ومع الخدمات الالكترونية التي تتضمنها الحكومة الالكترونية.

78 – 2- المتطلبات الإدارية:

إن توفير البنية التحتية لأنظمة المعلوماتية من أجهزة الحاسوب وتوفير خدمة الإنترنت في مؤسسات ووزارات الدولة ومدارسها وجامعاتها كلّها وفي مجال قطاع الأعمال لا يكفي بحد ذاته إذا لم يرافقه وعي من القيادات في الميادين كلّها بأهمية وجود مجهود الحكومة الالكترونية المنسق والاستعداد للتوافق مع مبادرات الحكومة الأردنية. الأمر الذي يعني تأهيل الكفاءات الإدارية على وجه التحديد وتدريب الموظفين جميعهم وتوعيتهم بمفهوم وأهمية الحكومة الالكترونية حتى يكونوا قادرين على نشر ثقافة الحكومة الالكترونية وترويجها لدى المتعاملين معهم.

79 – 3- المتطلبات القانونية والتشريعية:

وهي المتطلبات الأكثر أهمية وخطورة. وتنبع أهمية المتطلبات القانونية من كونها تشكل الإطار التنظيمي الوقائي الرادع الذي يحيط بكل متعلقات الحكومة الالكترونية، الأمر الذي يجعل التفكير بالتلاعب بمحتوى هذه الحكومة من قبل العابثين أمراً في غاية الصعوبة، وكذلك يضمن امن المعلومات وسريتها وخصوصيتها، خاصة للأفراد الذين يتملكهم الخوف من أن تصبح بياناتهم الخاصة ووثائقهم عرضة لاختراقها؛ وبالتالي تفقد حرمتها وخصوصيتها.

80 ـ أما خطورة المتطلبات القانونية التشريعية فهي تكمن في أن غيابها سيجعل الباب مفتوحاً على مصراعيه أمام المتطفلين والقراصنة ومجرمي المعلوماتية بكل أطيافهم للتطاول على محتوى الحكومة الالكترونية بكل ما تشمله، وقد يصل الأمر إلى حد التلاعب في الأرقام والبيانات خاصة في النواحي الاقتصادية المالية كما هو الحال في حالات الدفع الالكتروني عبر بوابة الحكومة الالكترونية (Electronic Payments) دون وجود إمكانية لمعاقبتهم لعدم وجود نصوص قانونية تسمح بذلك[1].

81 ـ وتجدر الإشارة إلى أن تطبيق مفهوم الحكومة الالكترونية في الولايات المتحدة الأمريكية ودول الاتحاد الأوروبي وغيرها من الدول الغربية كان متزامناً مع حملة لتعديل التشريعات القانونية القائمة خاصة الجنائية منها في خطوة الهدف منها الحماية القانونية الشاملة لهذا المفهوم وتخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات وأنظمتها[2]. فالعملية وحدة متكاملة فلا يمكن إيجاد

---

(1) الجرائم الالكترونية قد تنطلق من مناطق لا يوجد بها قوانين لمحاربة هذا النوع من الجرائم، كان هذا أحد الدروس التي قدمها فيروس (بقة الحب). فبالرغم من أن الفيروس انتشر في العالم أجمع والحق بالمؤسسات خسائر تقدر بملايين الدولارات إلا أن مخبرو مكتب التحقيقات الفدرالية وبعد أن تمكنوا من تحديد هوية مرتكب العمل وكان طالباً في الفلبين وجدوا أنه لا يوجد قانون يمكن من خلاله محاكمة الفاعل وبعد هذه الحادثة عمدت الفلبين إلى إصدار قوانين تجرم الأفعال التي ترتكب عبر الشبكات الالكترونية. يشار إلى أن فيروس بقة الحب أصاب حوالي 200 الف محور الكتروني عالمي من ضمنها مجلس العموم البريطاني والبيت الأبيض ووزارة الدفاع الأمريكية وشركة فورد وقواعد عسكرية امريكية والكثير من الشركات متعددة الجنسيات إلى الدرجة التي سمي بها الفيروس (بالقاتل القادم من مانيلا).

(2) الولايات المتحدة الأمريكية أصدر فيها الكونغرس الأمريكي قانون يسمى بالتحايل المعلوماتي في عام 1984 وكذلك أصدرت فرنسا في عام1978 قانون المعلوماتية والحقوق الشخصية، أعقب ذلك صدور مرسوم في عام 1981 بتحديد بعض المخالفات المرتبطة بمجال المعلوماتية ثم اصدرت في عام 1988 قانون لحماية نظم المعالجة الآلية للبيانات ثم اصدرت قانوناً جديداً عدل بعض أحكام قانون عام 1988 وذلك في 1994/3/1. مشار إلى ذلك عند الرومي، محمد أمين. جرائم الكمبيوتر والإنترنت، ط1، دار المطبوعات الجامعية، الاسكندرية، 2003، ص7.

في بريطانيا هناك قانون إساءة استخدام الكمبيوتر لعام 1990، وفي الدانمارك تم تعديل قانون العقوبات ليشمل جرائم المعلوماتية، اصدرت اليونان كذلك قانوناً خاصاً بجرائم الحاسوب، واصدرت وهولندا قانون جرائم الحاسوب لعام 1992و في ماليزيا تم إصدار قانون جرائم الحاسوب لعام 1997. وفي كندا تم إصدار قانون الدخول للمعلومات والخصوصية في عام 1982 وكذلك قانون حماية البيانات الشخصية والوثائق الالكترونية لعام 2000.

حكومة الكترونية دون وجود تشريعات تحكم هذه العملية من الناحية المدنية وكذلك من الناحية الجنائية.

وفي الأردن على وجه التحديد تم إقرار قانون المعاملات الالكترونية المؤقت رقم 85 لسنة2001 الذي قطع الجدل الذي كان دائراً حول حجية التوقيع الالكتروني، والوثائق الالكترونية في الإثبات وأضفى عليها طابعاً إلزاميا.

82 - وفي الواقع فإن الحماية المتكاملة للمعلوماتية من الجرائم التي قد تكون عرضة لها تتطلب تشريعات متناسقة يكمل بعضها بعضاً وتشمل جوانب الحياة الالكترونية كلّها[1] التي أصبحت تغزو مجتمعاتنا، حتى إن كان هذا الغزو ما زال في بدايته فالتشريعات القانونية قد تحمي من وقوع جرائم لو وقعت لسببت خسائر اقتصادية فادحة أو شكلت اعتداء صارخاً على حرمة الحياة الخاصة للأفراد وغير ذلك الكثير، وفي حال وقوع هذه الجرائم فان التشريعات القانونية ستكون لمرتكبي الجرائم المعلوماتية بالمرصاد.

---

(1) التشريعات القانونية فيما يتعلق بالجرائم المعلوماتية قد تتبلور شيئا فشيئا لتشكل فرعاً مستقلاً عن بقية الفروع القانونية الأخرى، هذا الفرع هو قانون الكمبيوتر (CIBYERLAW) والحقول التشريعية التي قد تندرج وتشكل قانون الكمبيوتر هي:

1- تشريعات الخصوصية أو قواعد حماية تجميع البيانات الشخصية ومعالجتها وتخزينها وتبادلها.
2- تشريعات جرائم الحاسوب التي تشمل جرائم الانترنت وشبكات الاتصال ضمن مفهوم اشمل هو مفهوم امن المعلومات والاعتراف للمعلومات بالحماية القانونية من الأنشطة كلّها التي يكون الحاسوب فيها هدفا أو وسيلة أو بيئة للجريمة.
3- تشريعات الملكية الفكرية في حقل حماية البرمجيات.
4- تشريعات الأصول الجزائية الإجرائية في مجال الضبط والتفتيش في بيئة الحاسب ومدى قابلية الحاسب للضبط و حجية المستخرجات الحاسوبية في الإثبات والأدلة الرقمية.
5- التشريعات المالية والمصرفية فيما يتصل بالمال الالكتروني وتقنيات الخدمات المصرفية والمالية وفي مقدمتها البطاقات المالية ونظم التمويل الالكتروني التي تطورت لتشمل أُطراً جديدة في حقل التوجه نحو الأتمتة الكاملة للعمل المصرفي والمالي (البنوك الالكترونية).
6- تشريعات التجارة الالكترونية (التعاقد الالكتروني، و التسوق الالكتروني وغير ذلك).
7- اتفاقيات ومعاهدات الاختصاص والقانون المطبق على المنازعات القضائية في بيئة الانترنت.

انظر، الموقع الالكتروني:
WWW.ARABCIN.NET/ARABIC/5NADWEH/PIVOT-7/ARABIC-ARRANGEMENT/.HTM

بعد هذا الاستعراض الموجز لمفهوم الحكومة الالكترونية وتداعيات تطبيقها على أرض الواقع نجد أن التطبيق الفعال والأمثل لهذا المشروع يستدعي إعطاء أهمية خاصة للتشريعات التي تحمي المعلوماتية من الجرائم التي قد تقع عليها. فتوجه الحكومة الأردنية نحو إقامة حكومة الكترونية هو من أهم الأسباب التي تستدعي الحماية الجنائية المتكاملة للمعلوماتية من الجرائم التي قد تقع عليها.

المطلب الثاني: أضرار الجرائم المعلوماتية على الاقتصاد الوطني

83 ـ "ما لم نستطع تأمين بنيتنا التحتية الالكترونية فان كل ما يحتاجه المجرم لتعطيل اقتصادنا ووضع حياتنا موضع الخطر هو نقرات بسيطة على جهاز الحاسوب والاتصال عن طريق الإنترنت. فالماوس (الفارة) يمكن أن يكون الآن أكثر خطورة من الرصاصة أو القنبلة".

هذا ما أدلى به (لامار سميث) رئيس اللجنة الفرعية المسؤولة عن الجريمة في الكونجرس الأمريكي للتدليل على الخسارة الاقتصادية التي قد تلحق الولايات المتحدة من جراء الجرائم المعلوماتية [1].

84 ـ والمؤشرات تبرز ازدياد خسائر الإجرام المعلوماتي خاصة في الدول التي تعتمد بشكل كبير على نظم التقنية المعلوماتية الأمر الذي يشكل تحديا كبيرا في مجال مواجهة هذه الجرائم ومكافحتها. إلا أن هناك صعوبة في وضع رقم محدد واضح المعالم لحجم الخسائر في مجال الجرائم المعلوماتية وهو ما يعبر عنه بالرقم الأسود.

---

(1) مناسبة هذا الحديث الذي أدلى به لامار سميث هو موافقة مجلس النواب الأمريكي بأغلبية ساحقة على قانون يسمح بتطبيق السجن مدى الحياة لمرتكبي الجرائم الالكترونية الشريرة. و كان الكونجرس الأمريكي قد وافق على ما يعرف بقانون الجرائم الالكترونية بغالبية 385 صوتاً مقابل 3 اصوات ويوسع هذا القانون من قدرات الشرطة في التصنت على الاتصالات عبر الانترنت دون الحصول على إذن مسبق من المحكمة، وكانت إدارة الرئيس الأمريكي بوش الابن قد طلبت من الكونجرس الموافقة على قانون تحسين الأمن الالكتروني طريقة للتعامل مع مشكلات القرصنة الالكترونية والإرهاب الالكتروني، وكان مشروع هذا القانون قد تم إعداده قبل هجمات 11 ايلول 2001 إلا أن الهجمات دعت الكونجرس إلى سرعة الموافقة عليه. انظر موقع، WWW.ALWATAN.COM .

85 ـ مدلول الرقم الأسود يشير إلى عدم التبليغ عن الجرائم المعلوماتية الأمر الذي من شأنه أن يخفي الرقم الحقيقي لها و يقلل من الشعور بمخاطرها وهذا يؤدي بدوره إلى وجود نسبة كبيرة من هذه الجرائم لا يتحقق العلم بوقوعها.

وقد دلت نتائج دراسة أجريت عام 1980 في فرنسا على أن الجرائم المعلوماتية التي تم الإبلاغ عنها للسلطات المختصة بلغت 15% فقط من مجموع الجرائم وان أدلة الإدانة لم تتوافر إلاّ لما نسبته خُمس النسبة المتقدمة أي ما يعادل حوالي 3% من مجموع هذه الجرائم المرتكبة. وتؤكد دراسة حديثة أجريت في الولايات المتحدة الأمريكية أن الرقم الأسود لجرائم الحاسوب والإنترنت يمثل الرقم الأكبر من حيث إجمالي هذه الجرائم و السبب الرئيسي لعدم إبلاغ المجني عليهم عن الجرائم المعلوماتية يرجع إلى خوف المجني عليهم من التعرض إلى الدعاية المضادة التي قد تنال من سمعتهم[1] كما سبق و اشرنا.

86 ـ كذلك يمثل الرقم الأسود نسبة الجرائم المعلوماتية التي يبلغ عنها ولكن لا يكتشف فيها الجاني أو لا تتوافر أدلة الإثبات فيها أو لا يلاحق الجاني فيها من الناحية القضائية مع العلم بوقوعها[2].

والدراسة التي قام بها معهد الحاسوب في سان فرانسيسكو الخاص بمكتب التحقيقات الفدرالي فرع جرائم الحاسوب عام 2003 على (520) مؤسسة أمريكية ووكالة حكومية تضع أمام أعيننا حجم الإضرار المالية التي تسببها الجرائم المعلوماتية. فقد وجدت الدراسة أن 88% من العينة التي أجريت عليها الدراسة كانوا ضحية جريمة معلوماتية، إذ أكد 64% من الذين شملهم البحث أنهم تعرضوا لسرقات معلوماتية إضافة إلى 24% عانوا من الأضرار التي لحقت بأجهزتهم بسبب الفيروسات ومن بين الذين يدركون حجم خسارتهم أوردوا أنهم خلال عام 1997 فقدوا (137) مليون دولار[3].

(1) محمود، مرجع سابق، ص80 ـ 81.

(2) محمود، مرجع سابق، ص81.

(3) انظر الموقع الالكتروني، WWW.ALYASSER.GOV.SA .

وتقدر خسائر الاقتصاد الأمريكي بسبب الجرائم المعلوماتية بـ (250) مليار دولار هذا بالإضافة إلى تعرض نظم المعلومات بوزارة الدفاع الأمريكية لمحاولات اختراق عديدة.

87 ـ والخسائر الاقتصادية الناجمة عن ارتكاب الجرائم المعلوماتية تزداد وتتضاعف عندما ترتبط بالجريمة المنظمة[1]. فالمنظمات الإجرامية لديها مهارة كبيرة في اكتشاف فرص القيام بأعمال ومشاريع جديدة غير مشروعة واستغلالها، والإنترنت والحاسوب والنمو المتواصل للتجارة الالكترونية حمل معه مجالات هائلة جديدة لتحقيق أرباح غير مشروعة.

وتتناسب الإنترنت باعتبارها شبكة تتخطى حدود البلدان مع هذا النمط الإجرامي ومع جهد هذه المنظمات الساعية لتحقيق أقصى الأرباح الأمر الذي يجعل النشاط الإجرامي باستخدام هذه الوسائل التقنية عملاً جذابا للغاية، إذ توفر الشبكة فرصا للقيام بمختلف أشكال السرقات سواء أكانت من المصارف الموصولة بالشبكة أو من الممتلكات الفكرية، وتؤمن وسائل لجرائم الاحتيال المعلوماتي. وشبكة الإنترنت باعتبار أنه يمكن استخدامها من دون معرفة الغير لشخص المستخدم يجعل منها قناة مثالية لتنفيذ العديد من نشاطات الجريمة المنظمة فالسرية تشكل عادة جزءاً رئيسياً من استراتيجية عمل هذه الجريمة[2]. والترابط بين الجريمة المنظمة و شبكة الإنترنت ترابط من المرجح له أن يزدهر وأن يتطور في المستقبل.

88 ـ ويمكن إعطاء الأمثلة الآتية على خطورة الجرائم المعلوماتية والخسائر المالية والاقتصادية التي قد تخلفها ورائها:

- في تشرين الأول/ أكتوبر عام 2000 ابتكرت مجموعة من حوالي 20 شخصاً بعضهم يرتبط بعائلات المافيا وبمساعدة شخص يعمل في بنك صقلية نسخة رقمية طبق الأصل لنظام اتصال البنك بشبكة الإنترنت، بعد ذلك قررت المجموعة استعمال هذه النسخة الرقمية المطابقة للأصل لتحويل مبلغ

(1) سيتم الحديث عن الجريمة المنظمة و تعريفها في المبحث الثالث من هذا الفصل ونحيل القارئ إليه منعاً للتكرار.

(2) انظر الموقع الالكتروني HTTP://USINFO.STATE.GOV.

(400) مليار دولار من البنك كان الاتحاد الأوروبي قد خصصها لتمويل مشاريع إقليمية في صقلية، وكان من المقرر غسل الأموال عبر مؤسسات مالية مختلفة مثل بنوك سويسرا، إلا أن الخطة باءت بالفشل عندما باح بالسر شخص من المجموعة إلى السلطات الرسمية[1]. وقد كشفت هذه المحاولة عن مدى الخسائر التي قد تسببها الجرائم المعلوماتية إذا تمت بنجاح.

- كذلك في أيلول 1999 تمكنت جماعة عرفت باسم أساتذة الهاتف تعمل انطلاقاً من الولايات المتحدة الأمريكية من الحصول على الآلاف من بطاقات إجراء المخابرات الهاتفية من شركة (SPRING) وبيعها، الأمر الذي كلف الشركة خسارة باهظة[2].

والدول العربية لم تكن بمنأى عن الجرائم المعلوماتية والخسائر الاقتصادية التي تسببها[3] وإن كانت خسائرها ليست بمقدار الخسائر التي تتكبدها الدول الغربية.

وتجدر الإشارة إلى أن مصر كانت من أوائل الدول الحريصة على محاربة الجرائم المعلوماتية حيث قامت وزارة الداخلية بإنشاء إدارة خاصة لمكافحة جرائم شبكات الحاسبات والنظم المعلوماتية وتختص الإدارة بالمتابعة اليومية للشبكات العاملة لضبط الحالات الخارجة عن القانون، والإجراءات تتخذ فوراً اتجاه المخالفين حيث يتم تدمير المواقع إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة.

وتجدر الإشارة إلى أن الخبراء الاقتصاديين أكدوا أن المنطقة العربية ستتعرض إلى أزمة خطيرة في الأعوام القليلة القادمة بسبب الإحجام عن استخدام الشبكات لتفعيل التجارة الالكترونية بين الدول العربية والأوروبية المتقدمة، وهذا الإحجام لم يكن وليد الصدفة فقد ساهمت الجرائم الالكترونية المعلوماتية وانتشار أشكالها

---

(1) انظر الموقع الالكتروني HTTP:// USINFO.STATE.GOV.

(2) الموقع الالكتروني السابق.

(3) تم اعتقال بريطاني يبلغ من العمر 32 عاماً ويعمل مهندساً في إحدى شركات المقاولات في دبي بعد اتهامه انه احد أعضاء جماعة كانت وراء محاولة تخريب شبكة الانترنت الإماراتية وقدرت خسائر الفترة التخريبية التي استمرت حوالي أسبوعين بملايين الدراهم وشلّت قدرة آلاف المستخدمين على البقاء في الشبكة لفترة طويلة الأمر الذي أصابهم بإحباط شديد. انظر الموقع الالكتروني:WWW.HABTOOR.COM .

خاصة مع تكرار سرقة بطاقات الائتمان في إضفاء حالة من الرعب على المؤسسات الاقتصادية العربية الضخمة وبدلا من معالجة الأخطاء وتفعيل القوانين وتفعيل وسائل الحماية والوقاية اكتفى الجميع بالجلوس في أماكنهم[1].

المطلب الثالث: عدم كفاية القوانين القائمة

89 ـ إذا كانت التشريعات العقابية التقليدية قد تناولت الجرائم التقليدية التي تقع على الأموال والأشخاص وغيرها بالتجريم، فإن هذه القوانين قد لا تطال غالبية الجرائم التقنية المعلوماتية بالتجريم لاختلاف الأخيرة عن سابقاتها في الطبيعة أو في الأركان أو في المحل.

وفي الواقع فإن القانون الجزائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري في تسخير المبتكرات للاستخدام السيئ[2].

90 ـ فالأشكال المستجدة للجريمة لم يعد يقتصر اعتداؤها على القيم المادية التي كانت محمية بقانون العقوبات، بل امتد هذا الاعتداء إلى القيم المعنوية مثل المعلومات والمعطيات وغير ذلك، فأصبحت النصوص التقليدية في قانون العقوبات عاجزة عن مواكبة هذه الأشكال المستحدثة من الإجرام المعلوماتي.

91 ـ من هنا فلا بد للمشرع الجنائي أن يتدخل ليتناول بالتجريم والعقاب ما يستجد من هذه الأشكال الإجرامية المعلوماتية التي لا تقع تحت سلطانه؛ وذلك تطبيقا لمبدأ شرعية الجريمة والعقوبة ويعني هذا المبدأ حصر مصادر التجريم والعقاب في نصوص القانون.

ولهذا المبدأ شقّان:

الأول: شرعية أو قانونية الجرائم، ويعني أن كل واقعة لا يمكن أن تعد جريمة ما لم يقرر القانون ذلك.

(1) انظر الموقع الالكتروني: WWW.ALRIVADH.COM.SA.

(2) الصغير، مرجع سابق، ص 18.

الثاني: شرعية أو قانونية العقوبات، ويعني أن المتهم لا يمكن أن يخضع لعقوبة تختلف عما يقرره المشرع، فالمشرع دون القاضي هو المختص بتحديد الأفعال التي تعد جرائم وبيان أركانها وعناصرها، وكذلك العقوبات المقررة لها من حيث نوعها أو مقدارها[1].

92 ـ النتيجة الأهم التي تترتب على مبدأ الشرعية هي التفسير الضيق لنصوص القانون الجنائي الذي يجب أن يلتزم به القاضي في مواجهة نقص النصوص أو في مواجهة النصوص التي تتسم بالغموض. ومبدأ الشرعية يحظر اللجوء إلى القياس على من يفسر نص التجريم، فلا يجوز للقاضي أن يقيس فعلاً ما لم يرد نص بتجريمه على فعل ورد نص بتجريمه، فيقرر للأول عقوبة الثاني للتشابه بين الفعلين، أو لكون العقاب على الثاني يحقق ذات المصلحة التي يحققها العقاب على الأول[2].

93 ـ في الواقع فان العلة وراء إقرار مبدأ شرعية الجريمة والجزاء هو انه يحمي الفرد حيال السلطة، حيث أن الإنسان لا يشعر بالأمان والطمأنينة إذا كان لا يعلم ما هي التصرفات المباحة وتلك المحظورة والعقوبات المقررة لها، كذلك فإن وجود نص قانوني يحدد الجرائم والجزاءات التي ستفرض على مرتكبيها يوجد قوة رادعة تزجر كل إنسان تدفعه نفسه نحو ارتكاب جريمة ما، وتجعله يفكر كثيرا قبل الإقدام عليها[3].

94 ـ ومن هنا فإنه يتوجب على المشرع الأردني إخضاع الجرائم المعلوماتية بنصوص صريحة مباشرة للعقاب خشية إفلات المجرمين من المساءلة الجنائية عن أفعال تتصف بالخطورة الكبيرة لما يترتب على إتيانها من اعتداء صارخ على الحياة الخاصة، والأسرار المهمة أحيانا والاعتداء على الذمة المالية للغير وغير ذلك الكثير من الصور الإجرامية، وما ينجم عنها من خسائر جسيمة تحل بضحاياها.

---

(1) المصدر السابق، ص 19 ـ 20.

(2) الصغير، مرجع سابق، ص21.

(3) صالح، نائل عبد الرحمن. محاضرات في قانون العقوبات (القسم العام)، ط1، دار الفكر للنشر، عمان، 1995، ص93.

وفي الواقع فان ترك مرتكبي الجرائم التقنية دون التصدي لأفعالهم الجرمية ومساءلتهم سيؤدي إلى فقد الثقة بالمؤسسات الحكومية التي تستخدم أجهزة الحاسوب والإنترنت وكذلك الشركات التجارية، وهذا بالفعل ما أدركته العديد من الدول التي اتجهت إلى وضع نصوص عقابية خاصة لمواجهة هذه الجرائم الحديثة و نصت على صورها صراحة[1]، ولم تترك الأمر إلى النصوص العقابية التقليدية التي لا يجوز القياس عليها في التجريم أو التوسع في تفسيرها تطبيقا لمبدأ شرعية العقوبة والجريمة.

95 ـ إنّ دور الفقه يأتي سابقاً لدور التشريع، فإذا كان القانون من العلوم الاجتماعية التي تتفاعل مع البيئة ولا يضع حلولا إلا لظواهر قد نشأت بالفعل حتى لا يأتي مجردا عن الواقع، فإن الفقه على خلاف ذلك عليه أن يسعى مبكراً للكشف عن الافتراضات والمخاطر المحتملة والممكنة، وعليه أن يحاول وضع الحلول لها بالاستعانة بالقانون المقارن وتجارب المجتمعات الأخرى، أو بالرجوع إلى مصادر العلوم المختلفة

---

(1) يمكن الإشارة إلى التجربة العمانية في هذا المجال حيث اصدرت سلطنة عمان المرسوم السلطاني 2001/72 حول تعديلات بعض أحكام قانون الجزاء العماني تضمن جرائم الحاسب وصورها. حيث يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين وبغرامة 1000 ريال إلى 5000 ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسوب في ارتكاب أحد الأفعال الآتية:

- الالتقاط غير المشروع للمعلومات أو البيانات.
- الدخول غير المشروع إلى أنظمة الحاسب.
- التجسس والتصنت على البيانات والمعلومات.
- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير بيانات أو وثائق مبرمجة أياً كان شكلها.
- إتلاف البيانات والمعلومات وتغييرها ومحوها.
- جمع المعلومات والبيانات وإعادة استخدامها.
- تسريب البيانات والمعلومات.
- التعدي على برامج الحاسب بالتعديل أو الاصطناع.
- نشر واستخدام الحاسب بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية

والمادة (276) مكرر يعاقب بالسجن مدة لا تزيد عن خمس سنوات و بغرامة لا تجاوز الف ريال كل من:

- قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب.
- استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك قبل بالدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك.
- مشار لهذا المرسوم السلطاني عند، الرومي، مرجع سابق، ص 7 ـ 8.

ومتابعة الاكتشافات العلمية الحديثة وما ينشأ عنها من مشكلات، أو ظواهر إجرامية ذلك كله في إطار معرفته ودرايته بالبيئة والمجتمع الذي يعيشه. ودور الفقه مهم جداً؛ إذ أنه المقدمة الطبيعية والمنطقية والعلمية التي يمكن أن يستنير بها المشرع عند سن القوانين بل و يهتدي بها القضاء[1].

(1) شحاتة، علاء الدين محمد. رؤيا أمنية للجرائم الناشئة عن استخدام الحاسب الآلي، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 453.

المبحث الثالث
المجرم المعلوماتي

96 ـ أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا إلا أنها في المقابل جلبت معها نسلاً جديداً من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

والمعلوماتية ينظر إليها دائما بوصفها أداة محايدة وأن مصدر ضعفها وانتهاكها هو الإنسان ذاته، والذي غالبا ما يهيئ فرصة استغلال الوسيلة المعلوماتية عن حسن أو سوء نية. فجوهر المشكلة يرتبط بالإنسان وشخصيته ودوافعه وكما هو معروف فإنه لا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم تضع في الاعتبار شخصية المجرم، والذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مرة أخرى مواطنا صالحا في مجتمعه[1].

97 ـ وتقترب سمات المجرم المعلوماتي في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء[2]. حيث أن كلا من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة المستوى ومن ذوي التخصصات والكفاءات العالية ويتمتعون بالذكاء وبالقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه، بل إن بعضهم يتمتع باحترام وثقة عالية من الأشخاص المحيطين بهم في مجال العمل أم في المحيط الاجتماعي.

وسوف أتناول في هذا المبحث دراسة شخصية المجرم المعلوماتي من حيث سماته وذلك في (المطلب الأول)، وأعرض بعد ذلك لأهم طوائف وفئات مجرمي المعلوماتية

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 33، 34.

(2) مصطلح المجرمين ذوي الياقات البيضاء مصطلح حديث نسبياً واول من اطلقه عالم الاجتماع (SutherLand) حيث وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة وتشمل انواعاً مختلفة من الجرائم كغسيل الاموال وتجارة الرقيق الأبيض وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم الفخمة.

www.minshawi.com/old/internetcrim-in%20the20%law.htm.

وذلك في (المطلب الثاني)، وأخيراً القي الضوء على أهم الدوافع التي قد تحمل المجرم المعلوماتي على ارتكاب جريمته وذلك في (المطلب الثالث).

المطلب الأول: السمات الخاصة با لمجرم المعلوماتي

98 ـ لم يكن لارتباط الجريمة المعلوماتية بالحاسوب والإنترنت أثراً على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثر أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين واتصافه بسمات معينة جعلت منه محلاً للعديد من الأبحاث والدراسات. ويتميز المجرم المعلوماتي بعدد من السمات والخصائص هي:

أولاً: المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء

99 ـ يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والإنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا. فتنفيذ الجريمة المعلوماتية يتطلب قدراً من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.

100 ـ إن المجرم المعلوماتي يمكن أن يكوّن تصوراً كاملاً لجريمته، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته، وذلك حتى لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها[1].

101 ـ يتميز المجرم المعلوماتي غالبا بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليه. فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء.

---

(1) قورة، مرجع سابق، ص52.

الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف[1] فالمجرم المعلوماتي يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها احد سواه و ذلك من اجل اختراق الحواجز الأمنية في البيئة الالكترونية ومن ثم نيل مبتغاه.

ثانياً: المجرم المعلوماتي يبرر ارتكاب جريمته

102 ـ يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[2].

103 ـ فهؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب، ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية قد انشأ مناخاً نفسياً موائماً لتصور استبعاد فكرة الخير والشر وقد ساعد على ذلك عدم وجود احتكاك مباشر بالأشخاص، ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل[3]. ففي كثير من الأحيان يقوم العاملون بالمؤسسات المختلفة باستخدام أجهزة الحاسوب لأغراض شخصية بوصفه سلوكاً شائعاً بين الجميع ولا ينظر إليه بوصفه فعلاً إجرامياً[4].

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 34.

(2) قورة. مرجع سابق، ص 54.

(3) الشوا، سامي، الغش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 525.

(4) يقول الأستاذ باركر وهو أحد أهم الباحثين الذين عنوا بالجريمة المعلوماتية بشكل عام وبالمجرم المعلوماتي بصفة خاصة "أن الفاعل في هذه الجرائم لا يتصور أن سلوكه يمكن أن يتصف بالإجرامي وان يستتبع ذلك توقيع العقاب عليه. فمن خلال لقائه بإثنين من المحكوم عليهم بسبب استعمال الحواسيب الخاصة برؤسائهم لأغراض شخصية وهو ما يندرج تحت جريمة الاستعمال غير المصرح به للنظام المعلوماتي ذكر المتهمان أن ما فعلاه هو سلوك شائع ومقبول في=

104 ـ إلا أن ذلك لا يعني أن عدم الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة كبيرة من مرتكبيها ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم وإدراك بعدم مشروعية وأخلاقية هذا الفعل، فهناك فئة لديها اتجاه إجرامي خطير وسوء نية واضح وهم على إدراك بخطورة أفعالهم.

ثالثاً: المجرم المعلوماتي إنسان اجتماعي

105 ـ المجرم المعلوماتي هو عادة إنسان اجتماعي قادر على التكيف في بيئته الاجتماعية بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله. فالمجرم المعلوماتي يتميز بأنه لا يضع نفسه في حالة عداء مع المجتمع الذي يحيطه بل إنه إنسان قادر على التوافق والتصالح مع مجتمعه.

فهو إنسان مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف ولا يعني ذلك تقليل من شأن المجرم المعلوماتي بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه[1].

106 ـ شعور المجرم أنه محل ثقة من مجتمعه وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.

رابعاً: خوف المجرم المعلوماتي من كشف جريمته

107 ـ يتصف مجرمو المعلوماتية بالخوف من كشف جرائمهم وافتضاح أمرهم، وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان.

=المؤسسة التي يعملان بها وأن العاملين في المؤسسة يقومون باستخدام النظام لأغراض شخصية بعضها لتحقيق ربح مادي والبعض الآخر لمجرد التسلية في أوقات الفراغ" انظر، قورة، مرجع سابق، ص 55

(1) انظر، الرومي، مرجع سابق، ص23.

108 ـ ويساعد مجرمي المعلوماتية على الحفاظ على سرية أفعالهم طبيعة الأنظمة المعلوماتية نفسها؛ ذلك أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعه لا يمكن التنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى وهو ما يساعد على عدم كشف الجريمة طالما أن جميع خطوات التنفيذ معروفة مسبقاً حيث لا يحتمل أن تتدخل عوامل غير متوقعه يكون من شأنها الكشف عن الجريمة[1].

109 ـ وهذه الخشية لدى مجرمي المعلوماتية من اكتشاف أفعالهم مردها انتماؤهم في الغالب الأعم إلى وسط اجتماعي متميز، سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل.

110 ـ أثبتت الدراسات أن غالبية مرتكبي الجرائم المعلوماتية غير قادرين على ارتكاب الجرائم التقليدية خاصة تلك التي تتطلب مواجهة مع المجني عليه فالمجرم المعلوماتي لا يستطيع الاعتداء على المجني عليه بطريقة مباشرة إلا انه لا يرى غضاضة في أن يكون هذا الاعتداء عن طريق البيئة الالكترونية[2].

خامساً: المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي

111 ـ ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها.

(1) قورة، مرجع سابق، ص 56.

(2) هذا ما توصل له الأستاذ باركر خلال دراسته للأنماط المختلفة لمجرمي المعلوماتية. انظر، المصدر السابق، ص 56.

وقد تتمثل هذه السلطة في الحق في: استعمال الأنظمة المعلوماتية، أو إجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة[1].

المطلب الثاني: فئات مجرمي المعلوماتية

112 ـ إن التسارع المذهل الذي يشهده عالم المعلوماتية والتقنيات الرقمية الحديثة انعكس بدوره على الجرائم التي ترتكب في البيئة التقنية الالكترونية فأصبحنا أمام جرائم مستحدثة سريعة التطور، مرتكبوها ماهرون في ابتكار الأساليب الحديثة لخرق الحواجز الأمنية في هذا العالم الرقمي مستخدمين خبراتهم ومهاراتهم الذهنية والعقلية.

113 ـ وأمام هذا التطور والتغير السريع في أنماط الجريمة المعلوماتية وصورها فقد يكون من الصعب وضع تصنيف ثابت لطوائف مجرمي المعلوماتية، ولكن يمكن لنا وفقا لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين بعض هذه الأنماط لهؤلاء المجرمين. ولكن لا بد من الإشارة أولا إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة.

الفئة الأولى: صغار مجرمي المعلوماتية

كما يسميهم البعض صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها[2].

114 ـ وقد تباينت الآراء بالنسبة لهذه الطائفة، حيث يرى البعض أنه: "لا يبدو من المناسب أن نصنف هؤلاء الشباب في طائفة أو أخرى من الطوائف الإجرامية لان لديهم ببساطة ميلاً للمغامرة والتحدي والرغبة في الاكتشاف ونادراً ما تكون أهداف أفعالهم

(1) قورة، مرجع سابق، ص 53.

(2) الشوا، ثورة المعلومات وانعكاساتها...، مرجع سابق، ص39.

المحظورة غير شريفة وهم لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية "[1].

115 ـ بينما هناك اتجاه آخر يناصر هذه الفئة ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخيار ويتمادى هذا الاتجاه في تقديره لهذه الفئة باعتبارهم لا يسببون ضرراً للنظام ولا يقومون بأعمال احتيال وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات[2].

116 ـ أما الاتجاه الأخير فيرى أن هذه الطائفة تصنف ضمن مجرمي المعلوماتية مثل غيرهم من المجرمين[3]. حيث أن أفعالهم المتمثلة في انتهاك الأنظمة واختراق الحواجز الأمنية في البيئة الالكترونية تعد أفعالاً خطيرة من الناحية العملية، بل إن أفعالهم لا تقف عند حدود دولة ما بل إنها تتعدى الحواجز الجغرافية.

117 ـ وفي الواقع فإنه يجب عدم التقليل من خطورة هؤلاء الأشخاص فهذه الفئة قد تتعدى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في مجال ارتكاب الجرائم المعلوماتية وهي مرحلة الاحتراف لهذه الجرائم[4]. كما أن هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها من أجل تحقيق مآربهم وغاياتهم الإجرامية من خلال التقنيات الرقمية.

حيث أن هذه الفئة تكون أكثر تقبلاً لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والإثارة والتحدي في طياتها[5].

---

(1) انظر في ذلك، المصدر السابق، ص40.

(2) انظر، عرب، دليل أمن المعلومات... مرجع سابق، ص286.

(3) انظر، عرب، دليل امن المعلومات... مرجع سابق، ص286.

(4) للتدليل على خطورة افعال هذه الفئة نذكر على سبيل المثال تلاميذ المدرسة الثانوية في ولاية ما نهاتن الذين استخدموا عام 1980 طرفيات غرف الدرس للدخول إلى شبكة اتصالات ودمروا ملفات زبائن الشركة في هذه العملية.

(5) حجازي، الاحداث والانترنت... مرجع سابق، ص56.

الفئة الثانية: القراصنة

118 ـ قراصنة المعلومات هم عادة مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة. ويمكن تصنيف القراصنة إلى صنفين هما:

1- القراصنة الهواة العابثون أو (الهاكرز) Hackers:

119 ـ هذا القسم من القراصنة أو ما اصطلح على تسميتهم "بالهاكرز" يرون في اختراق الأنظمة المعلوماتية تحدياً لقدراتهم الذاتية. وهذه الطائفة غالباً ما تكون من هواة الحاسوب؛ فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحياناً أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحياناً أخرى[1]. وهم يدعون انه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول. ومجرمو المعلوماتية من هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الالكترونية[2].

فعلى سبيل المثال خرق استشاري تقنية معلومات أحد الأنظمة الأمنية لشبكة الإنترنت البريطانية لمجرد كشف الفجوات الأمنية بها وقد نجح في الحصول على أسماء لأكثر من (24) ألف شخص وعناوينهم وكلمات السر ومعلومات البطاقات الائتمانية من بينهم خبراء عسكريون وموظفون حكوميون وكبار مديري الشركات[3].

120 ـ وهناك القراصنة الأخلاقيون الذين يقولون أنهم يعملون من أجل المصلحة العامة، فشكلوا لهم منظمات خاصة مثل منظمة القراصنة ضد مواقع إباحية الأطفال

(1) الزيدي، مرجع سابق، ص 40.

(2) محمود، مرجع سابق، ص 45.

(3) في مقابلة سرية أجرتها صحيفة التايمز مع هذا القرصان قال "إن اختراق الموقع الأمني مسألة سهلة جداً فهي اشبه بمن يبحث عن مفتاح معين في مجموعة صناديق ثم يجد أمامه بوابة جانبية مفتوحة على مصراعيها. انظر الموقع الالكتروني www.habtoor.com .

التي استطاعت القيام بحملات تأديبية لتعطيل قدرة بعض المواقع الالكترونية عن عرض مواد غير أخلاقية[1].

121 ـ وفي الحقيقة هناك سمة مميزة لهذه الفئة من القراصنة ألا وهي تبادلهم للمعلومات فيما بينهم وتحديداً التشارك في وسائل الاختراق وآليات نجاحها في مواطن الضعف في نظم الحاسوب والشبكات خاصة عن طريق النشرات الإعلامية الالكترونية ومجموعات الأخبار.

122 ـ إلا أن الحقيقة التي يجب أن لا نخفيها هي أن هؤلاء القراصنة الهواة ساهموا في كشف الفجوات الأمنية للأنظمة المعلوماتية في المؤسسات المالية وغيرها الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي قد يقوم بها مجرمو المعلوماتية.

ويشاع في بعض المنشآت التي يضبط بها أحد قراصنة المعلومات أن يتم إلحاقه بالفريق المعلوماتي المكلف بأمن النظام المعلوماتي فيها[2].

2- القراصنة المحترفون (Crackers):

123ـ هذه الفئة تعكس اعتداءاتهم ميولاً إجرامية خطرة تنبئ عن رغبتها في إحداث التخريب[3]. و يتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون إضراراً كبيرة.

وعادة ما يعود المجرم المحترف بالجريمة المعلوماتية إلى ارتكاب الجريمة مرة أخرى حيث تزداد سوابقه القضائية وهو يعيش لسنوات طويلة من عائد جرائمه، وهذا المجرم لا يفضل الأفكار المتطرفة وإنما الأفكار التي تدر عليه الأرباح الشخصية[4].

---

(1) الموقع الالكتروني السابق.

(2) الشوا، ثورة المعلومات... مرجع سابق، ص 36.

(3) عرب، دليل أمن المعلومات... مرجع سابق، ص 286.

(4) محمود، مرجع سابق، ص 56.

124 ـ توضح الدراسات التي أجراها معهد (Stand Ford Research) أن محترفي الجرائم المعلوماتية من الجيل الحديث هم غالباً من الشباب الذين تتراوح أعمارهم من 25 إلى 45 سنة و تبين الإحصاءات في هذا المجال ما يلي:[1]

- أن 25 % من أفعال الغش المعلوماتي أو الجريمة المعلوماتية يرتكبها المحلل.
- أن 18 % من هذه الأفعال يرتكبها المبرمج.
- أن 17 % يرتكبها المستخدم الذي لديه أفكار خاصة بنظم المعلومات.
- وان 12% يرتكبها الشخص الأجنبي عن المكان الذي تتواجد فيه نظم المعلومات.
- وان 11% من هذه الأفعال يرتكبها فني التشغيل.

الفئة الثالثة: الموظفون العاملون في مجال الأنظمة المعلوماتية

125 ـ بحكم طبيعة عمل هؤلاء الموظفين ونظراً لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظراً للمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية، وأهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكابه للجريمة المعلوماتية أسهل نظرا للثقة التي يتمتع بها.

وهناك فئة من الموظفين الحاقدين على عملهم أو على مؤسساتهم الذين قد يقومون بأفعال إجرامية لا تهدف إلى الكسب المادي بل هدفها الانتقام والثأر من أصحاب عملهم وهذه الفئة يذهب البعض إلى تسميتها " بفئة مجرمي المعلوماتية الحاقدين"[2].

الفئة الرابعة: مجرمو المعلوماتية أصحاب الآراء المتطرفة

126 ـ تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون

(1) محمود، مرجع سابق، ص 56. وانظر كذلك، الشوا، ثورة المعلومات... مرجع سابق، ص 42، 43.

(2) عرب، دليل امن المعلومات... مرجع سابق، ص 283. انظر كذلك، محمد، سليمان مصطفى، (1999). جرائم الحاسوب وأساليب مواجهتها. مجلة الأمن والحياة. العدد (199)، ص50.

في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي ويتركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه. وبدأ اهتمام هذه الجماعات وخاصة تلك التي تتمتع بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية(1).

127 ـ فهذه الجماعات تدافع عن قضية أو معتقد معين ولا تهدف ابتداء إلى تحقيق الربح المادي، وفي هذا تختلف هذه المنظمات المتطرفة عن المنظمات الإجرامية المنظمة، حيث تهدف الأخيرة إلى تحقيق مصالحها الشخصية المباشرة وتحديداً تحقيق الربح المادي.

128 ـ قامت جماعات تنتمي إلى منظمات إرهابية دولية من اليمين المتطرف واليسار مثل جماعة الألوية الحمراء الايطالية ومنظمة (LECLODO) وهي: منظمة فرنسية متخصصة في تدمير نظم المعلومات وغيرها من المنظمات الأخرى بارتكاب أفعال اعتداء على أنظمة المعلومات المنتشرة في أوروبا ابتداء من عام 1978.

وقد تعرضت وزارات وجامعات ومؤسسات مالية لهجمات الألوية الحمراء، ومن هنا أيقنت المنظمات الإرهابية أن في استطاعتها بمجهود بسيط أن تلحق أضرارا ضخمة داخل أي مشروع عن طريق تدمير المركز المعلوماتي له؛ لذا أصدرت الألوية الحمراء في فبراير 1998 منشورا شرحت فيه إستراتيجيتها وأهدافها من الهجوم على النظم المعلوماتية (2).

الفئة الخامسة: مجرمو المعلوماتية في إطار الجريمة المنظمة

129 ـ في عالم الشبكات الالكترونية – كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، وقد يكون أفضل ما

---

(1) فورة، مرجع سابق، ص 58.

(2) ويبدأ المنشور الذي أصدرته الألوية الحمراء بالتعريف بالمحور الاستراتيجي للمنظمة وهو مهاجمة الهيئات متعددة الجنسيات و تقصد الألوية الحمراء بالهيئات متعددة الجنسيات تلك الموجودة على وجه الخصوص في الولايات المتحدة الأمريكية فهي عدوها الأول و تعزو المنظمة إلى أجهزة الحاسوب نجاح هذه الهيئات ويعتبرون الحاسوب سلاحاً خطيراً بفضل قدرته على حفظ المعلومات ومقارنتها. أنظر، محمود، مرجع سابق، ص 66،67.

توصف به هذه الأعمال أنها جرائم غير منظمة. إلا أن مجموعات الجريمة المنظمة بدأت بشكل متزايد باستغلال الفرص الجديدة التي يوفرها العالم الرقمي.

130 ـ ومن التعريفات التي قيلت في الجريمة المنظمة أنها: "تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته آلاف المجرمين الذين يعملون وفقاً لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطوراً وتقدماً، كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم وتفرض أحكاما بالغة القسوة على من يخرج عن ناموس الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة"[1].

وعرفت هذه الجريمة كذلك من قبل الوفد المصري في المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين أنها: "مشروع إجرامي يمارسه مجموعة من الأفراد بتنظيم مؤسس ثابت له بناء هرمي ومستويات للقيادة ومستويات للتنفيذ وفرص للترقي ويحكمه نظام داخلي صارم ويستخدم الإجرام والعنف والتهديد والابتزاز والرشوة في إفساد المسؤولين وفرض السطوة بهدف تحقيق أرباح طائلة بوسائل غير مشروعة، حتى ولو اتخذ قالباً شرعياً من الناحية القانونية"[2].

131 ـ فالجريمة المنظمة تسعى في المقام الأول إلى الإفادة المادية أو تحقيق الأرباح الطائلة من خلال مواصلة العمل عبر وسائل إجرامية متنوعة، وهذه الجريمة تعد من جرائم ذوي النفوذ والسلطان التي قد يتورط فيها رجال السياسية وأصحاب المناصب الرفيعة فهي تعد بالفعل من جرائم ذوي الياقات البيضاء.

132 ـ منظمات الجريمة المنظمة تطور أساليب عملها باستمرار بما يحقق أهدافها وغاياتها، والعوامل المساعدة في تطوير هذه المنظمات لطرق عملها الموائمة المالية والاقتصادية التي تتمتع بها، فهي تسعى دوماً إلى استغلال الوسائل التقنية الحديثة في

---

(1) هذا التعريف للفقية (أوجيت ناكواي) مشا ر له عند، حجازي، الاحداث والانترنت... مرجع سابق، ص 62.

(2) اعمال مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين والذي عقد بالقاهرة في (1995). تقرير جمهورية مصر العربية. مشار له عند، حجازي، الاحداث والانترنت... مرجع سابق، ص 64.

القيام بنشاطاتها، فاستفادت هذه المنظمات عبر سنوات عملها من أحدث وسائل الاتصال حتى تؤمن الترابط بين أفرادها وجماعاتها.

وسعت وتسعى هذه المنظمات إلى الاستفادة من أجهزة التقنية المعلوماتية الحديثة المتمثلة في جهاز الحاسوب وشبكة الإنترنت لتسوية أعمالها وتسهيل تنفيذها؛ فلقد وجدت هذه المنظمات في شبكة الإنترنت وسيلة لا تضاهى للقيام بعمليات غسيل الأموال على نطاق واسع وكذلك لتدعيم تجارة الرقيق الأبيض وتجارة الأعضاء البشرية عبر إنشاء مواقع خاصة بهذه الأعمال. وهذه التقنيات الحديثة تتناسب مع طبيعة النشاطات الإجرامية لجماعات الجريمة المنظمة التي تعد من الجرائم العابرة للحدود.

133 ـ تقوم جماعات الجريمة المنظمة بتبني أصحاب الكفاءات وأصحاب الخبرة والموهوبين في مجال تقنية المعلومات، وذلك بإغرائهم بالمال لينضموا إلى صفوفها وتقوم بتدريبهم وزيادة مهاراتهم في هذا المجال لخلق مجرمين متخصصين في الجرائم المعلوماتية في إطار هذه المنظمات. ويمارس مجرمو المعلوماتية في نطاق هذه المنظمات نشاطات تدر على المنظمة أرباحاً هائلة فيقومون بتزوير البرامج وتقليدها واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى العالمية، كما يمارسون أعمال التجسس الصناعي والتجاري.

134 ـ الجرائم المعلوماتية تشكل عامل جذب كبير لهذه المنظمات الإجرامية فبالإضافة إلى الأرباح المادية المرتفعة التي تنتج من هذه الجرائم فإن صعوبة الكشف عنها وصعوبة إثباتها

بالمقارنة مع الجرائم التقليدية، كذلك فإن البطء في التحقيق في هذه الجرائم نتيجة لعدم التعاون الدولي الكافي في هذا المجال جعل منها مادة إجرامية دسمة تغري هذه الجماعات باقترافها.

135 ـ تجدر الإشارة إلى أن نسبة هذا النمط من الجرائم المعلوماتية التي تدخل في إطار الجريمة المنظمة ما زالت منخفضة بالمقارنة بالأنماط الأخرى ويرجع ذلك بصفة

أساسية لما تتطلبه هذه الجريمة من توافر درجة عالية من المعرفة والخبرة بتقنيات الحاسوب والإنترنت[1].

المطلب الثالث: الأسباب الدافعة لارتكاب الجرائم المعلوماتية

136 ـ الباعث أو الدافع هو: "العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام"[2].

أشار المشرع الجزائي الأردني في المادة 67 إلى تعريف الدافع (الباعث) بقوله:

(1. الدافع هو العلة التي تحمل الفاعل على الفعل أو الغاية القصوى التي يتوخاها.

2. لا يكون الدافع عنصراً من عناصر التجريم إلا في الأحوال التي عينها القانون)[3].

137 ـ يتضح من هذا النص أن الباعث أو الدافع لا يعتبر عنصراً من عناصر الجريمة إلا في الأحوال التي يحددها القانون. فالجريمة تقوم بتحقق عناصرها وأركانها أيا كان الباعث من وراء ارتكابها. والبواعث أو الدوافع التي قد تدفع المجرم المعلوماتي إلى ارتكاب جريمته تتنوع وأهم هذه الدوافع هي:

أولاً: الرغبة في التعلم

138 ـ الرغبة الشديدة في تعلم كل ما يتعلق بأنظمة الحاسوب والشبكات الالكترونية قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية ويشير الأستاذ (ليفي) مؤلف كتاب قراصنة الأنظمة إلى أخلاقيات هؤلاء القراصنة التي ترتكز على مبدأين أساسيين:

1- إن الدخول إلى أنظمة الحاسوب يمكن أن يعلمك كيف يسير العالم.

---

(1) قورة، مرجع سابق، ص58.

(2) السعيد، كامل، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، ط2، دار الفكر للنشر والتوزيع، عمان، 1983، ص 226.

(3) قانون العقوبات الأردني، قانون رقم 16 لسنة 1960 والمعدل بالقانون المؤقت رقم 54 لسنة 2001 والمعدل بالقانون المؤقت رقم 86 لسنة 2001.

2- إن عملية جمع المعلومات يجب أن تكون غير خاضعة للقيود[1].

139 ـ هناك من يرتكب جرائم الحاسوب؛ بغية الحصول على الجديد من المعلومات وسبر أغوار هذه التقنية المتسارعة النمو والتطور. وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية لأنظمة الحاسوبية[2].

140 ـ بشكل عام يرى هؤلاء المجرمون أن جميع المعلومات المفيدة يجب أن تتاح حرية نسخها والاطلاع عليها، إلا أنهم يقرون بضرورة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعضها خاصة بعض المعلومات السرية التي تخص الأفراد[3].

ثانياً: الدوافع المادية "الربح وكسب المال"

141 ـ الرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم. من أجل تحقيق المكاسب المالية هذه يتم اللجوء إلى ارتكاب الجريمة المعلوماتية أما عن طريق المساومة على البرامج أو المعلومات المتحصلة بطريق الاختلاس من جهاز الحاسوب أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية وغير ذلك الكثير، ولقد أشارت مجلة (Securite inform atiqne) وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال و23% من أجل سرقة معلومات و19% أفعال إتلاف و 15% سرقة وقت الآلة أي الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية[4].

---

(1) انظر، محمود، مرجع سابق، ص69.

(2) المصدر السابق، ص70.

(3) انظر، محمود، مرجع سابق، ص 69.

(4) الرومي، مرجع سابق، ص 24.

142 ـ تجدر الإشارة إلى أنه في حال نجاح المجرم في ارتكاب جريمته المعلوماتية فإن ذلك قد يدر عليه أرباحاً تكون هائلة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة لاقترافه هذا النوع من الإجرام من خلال ما يرويه أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا[1] بقوله:

(لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن أكرر ذلك في أي وقت لقد كان شيئا سهلاً فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني).

ثالثاً: المتعة والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات

143 ـ اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه، ويمكن لنا أن نوضح هذا الأمر من خلال ما ذكره أحد قراصنة الحاسوب:

"كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى البيت بعد يوم آخر في المدرسة وأدير تشغيل جهاز الحاسوب وأصبح عضوا في نخبة قراصنة الأنظمة. كان الأمر مختلفاً برمته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط، في البدء كنت أسجل اسمي في لوحة النشرات الخاصة حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد وبعد ذلك ابدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة، وأنسى جسدي تماما بينما أتنقل من جهاز حاسوب إلى آخر محاولا العثور على سبيل للوصول إلى هدفي، لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل

(1) مشار إلى هذه الواقعة عند، محمود، مرجع سابق، ص 57.

شيء غير قانوني وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات. كنت على حافة التكنولوجيا واكتشاف ما وراءها واكتشاف الكهوف الالكترونية التي لم يكن من المفترض وجودي بها"[1].

144 ـ على صعيد آخر قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة في قهر الأنظمة الالكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة.

فمجرمو المعلوماتية يتملكهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية ففي بعض الأحيان وجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي. وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها وقد يندفع تحت تأثير رغبة قوية من اجل تأكيد قدراته التقنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية[2].

رابعاً: الرغبة في الانتقام

145 ـ الباعث على ارتكاب الجريمة المعلوماتية قد يكون الرغبة في الانتقام من شخص ما أو مؤسسة ما أو حتى من بعض الأنظمة السياسية في بعض الدول أو الانتقام من رب العمل.

فعلى سبيل المثال، دفع الانتقام بمحاسب شاب إلى أن يتلاعب بالبرامج المعلوماتية بحيث تختفي كل البيانات الحسابية الخاصة بديون هذه المنشأة بعد رحيله بعدة أشهر وقد تحقق هذا الأمر في التاريخ المحدد[3]

(1) انظر، محمود، مرجع سابق، ص 73، 74.

(2) الشوا، ثورة المعلومات... مرجع سابق، ص 53.

(3) الشوا، ثورة المعلومات... مرجع سابق، ص 52. انظر كذلك حول الرغبة في الانتقام من رب العمل، عرب، يونس، (1994). جرائم الحاسوب، رسالة ماجستير، الجامعة الأردنية، عمان، الأردن، ص109.

خامساً: دوافع أخرى

146 ـ الدوافع السابقة ليست هي الوحيدة بل إن هناك دوافع أخرى تدفع لارتكاب الجريمة المعلوماتية.

147 ـ فمثلاً التنافس السياسي والاقتصادي قد يكون دافعا إلى ارتكاب هذه الأفعال، فقد قام بعض القراصنة المتواجدين على الأراضي الروسية باختراق نظم حاسبات حكومية في الولايات المتحدة الأمريكية مدة عام كامل، حيث قاموا بسرقة معلومات غير سرية ولكنها حساسة من أجهزة الحواسيب العسكرية الأمريكية.

148 ـ كما يعّد التسابق الفضائي والعسكري بين الدول دافعا لهذه الجريمة، فقد قام القراصنة بالإغارة على شبكات معلوماتية تابعة لوكالة الفضاء ناسا ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية[1].

149 ـ كما أن مناهضة العولمة قد تكون إحدى الدوافع لارتكاب هذا الفعل، فقد تم اختراق النظام المعلوماتي للمنتدى الاقتصادي العالمي في دافوس بسويسرا، وتمت عملية سرقة معلومات سرية تتعلق بعدد من الشخصيات الثرية المؤثرة التي شاركت في المؤتمر وأرسلت إلى إحدى الصحف السويسرية[2].

كما وجدت مجموعات تطلق على نفسها مجموعات الكراهية على الإنترنت تزدري كل القيم الدينية والأخلاقية والاجتماعية السائدة في المجتمعات وبصفة خاصة تلك المرتبطة بالأسرة. وهناك مواقع الإلحاد التي تطالب بإلغاء الدين والدولة والأسرة وتحرير الإنسان من تلك الأصفاد والقيود[3]. وهؤلاء جميعا قد يرتكبون أفعالاً إجرامية معلوماتية تبدو وفقاً لآرائهم ومعتقداتهم مشروعة وتهدف إلى تحسين العالم.

(1) كان من جراء ذلك ان قام البنتاجون بإنشاء "مركز الحرب المعلوماتية" للدفاع عن الولايات المتحدة الأمريكية ضد القراصنة وتحديد وسائل الهجوم على شبكات حاسب الاعداء. انظر. أحمد. الجوانب الموضوعية... مرجع سابق، ص21، 22.

(2) www.news.bbc.co.uk/hi/arabic/news/newsied1153000/1153/24.stm.

(3) انظر، احمد، الجوانب الموضوعية والإجرائية... مرجع سابق، ص 24.

150 ـ كما أن المنافسة التجارية أو التجسس العسكري أو الصناعي قد يكون من البواعث التي قد تدفع إلى ارتكاب الجرائم المعلوماتية ليس من قبل الأفراد فحسب بل من قبل الدول أيضا.

الفصل الثاني

الجرائم المعلوماتية الواقعة على النظام المعلوماتي

الفصل الثاني
الجرائم المعلوماتية الواقعة على النظام المعلوماتي

151 ـ تناولت في الفصل التمهيدي من هذه الدراسة مكونات النظام المعلوماتي التي تشمل المكونات المادية والمكونات المنطقية (المعنوية). والجرائم الواقعة على النظام المعلوماتي التي تقع على الشق المادي للنظام أو على الشق المنطقي (المعنوي).

وقوع الجريمة على المكونات المادية للنظام المعلوماتي:

152 ـ الاعتداء على المكونات المادية للنظام المعلوماتي يتحقق إذا كان الحاسوب والأجهزة الملحقة به أو الشبكات المعلوماتية محلاً للاعتداء.

وتقوم الجريمة في هذه الحالة بإتيان أفعال مادية قد يكون من شأنها إخراج الحاسوب من حيازة مالكه بغية إدخاله في حيازة شخص آخر وهو الأمر الذي يتم في بعض الجرائم الواقعة على الأموال. وقد يتحقق وقوع بعض هذه الجرائم بإتلاف الأجهزة وتدميرها أو بحرقها وغير ذلك من الأفعال المجرمة.

وهذه الجرائم هي جرائم تقليدية وبالتالي يسأل مرتكبها بموجب النصوص العقابية الجنائية القائمة في قانون العقوبات الأردني. وتجدر الإشارة إلى أن حالات الاعتداء على المكونات المادية للنظام المعلوماتي لا تثير إشكالات في الواقع العملي؛ نظراً لأن هذه المكونات تعتبر مالاً مادياً منقولاً يخضع للحماية الجنائية بموجب نصوص قانون العقوبات.

وقوع الجريمة على المكونات المنطقية (المعنوية) للنظام المعلوماتي:

153 ـ تقوم الجريمة المعلوماتية إذا كانت المكونات المنطقية للنظام المعلوماتي ممثلة بالمعلومات بكلِّ صورها هي محل الاعتداء. فقد يتم سرقة هذه المعلومات أو إتلافها أو تدميرها أو تزويرها والعبث بها وغير ذلك من الأفعال غير مشروعة.

وفي هذه الحالة تبدو النصوص القائمة في قانون العقوبات الأردني قاصرة عن تحقيق الحماية الكافية والمتكاملة للمعلومات، وذلك لأن القانون الجنائي في الأردن في أغلب الدول العربية يعاني من فراغ تشريعي في المجال المعلوماتي.

154 ـ وحيث أن الجرائم الواقعة على المكونات المادية للنظام المعلوماتي لا تثير أية مشكلة قانونية كونها مشمولة بالحماية الجزائية، فإننا سنقوم في هذا الفصل بتناول أبرز الجرائم المعلوماتية الواقعة على المكونات المنطقية (المعنوية) للنظام المعلوماتي وذلك في أربعة مباحث على النحو الآتي:

المبحث الأول: سرقة المعلومات.

المبحث الثاني: الاستعمال غير المصرح به للنظام المعلوماتي.

المبحث الثالث: إتلاف المعلومات.

المبحث الرابع: تزوير المعلومات.

المبحث الأول
سـرقـة المـعـلـومـات

155 ـ أصبحت المعلومة مصدر قوة ومصدر سلطة حتى قيل إن المعرفة هي سلطة وإن الحصول على المعرفة وحسن استخدامها عاملان أساسيان من عوامل التقدم، ولذلك فإن التكنولوجيا الحديثة تتعلق بالمعرفة ثم السلطة[1].

156 ـ نظراً لما تشغله المعلومات من قيمة اقتصادية كبيرة كان هناك تهافت من قبل الأفراد والمؤسسات المختلفة وكذلك الدول للحصول عليها من أجل تسريع عملية التقدم في كلّ المجالات. وبالمقابل كانت هناك طائفة متواجدة دائماً للقيام بالاستغلال غير المشروع لهذه المعلومات وبكل الأساليب المتاحة أمامها. وسرقة المعلومات ـ المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكة العالمية للمعلومات (الانترنت) ـ هي إحدى أكثر الأساليب انتشاراً في مجال الاعتداء على المعلومات. ويطلق البعض على هذه الجريمة: "جريمة قرصنة المعلومات"[2] وتجري عملية السرقة من خلال وصول الأفراد غير المرخص لهم إلى المعلومات والبيانات وبرامج الحاسوب.

ويقصد بالقرصنة المعلوماتية (نسخ البرامج على نحو غير مشروع أو الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة أو غير مباشرة)[3] وعمليات القرصنة المعلوماتية ينتج عنها خسائر كبيرة جداً، فعلى سبيل المثال تسببت عمليات النسخ غير القانوني للبرامج بخسائر قدرت عام (2000) في عموم العالم بـ

(1) حسبو، عمرو، حماية الحريات في مواجهة نظم المعلومات، ط1، دار النهضة العربية، القاهرة، 2000، ص30. وكذلك انظر، الكساسبة، يوسف، (2001). التطور التقني وتطور الجريمة. مجلة الأمن والحياة. العدد (227). ص42.

(2) الزيدي، مرجع سابق، ص32.

(3) شتا، محمد، الحماية الجنائية لبرامج الحاسب الآلي، ط1، دار الجامعة الجديدة للنشر، القاهرة، 2001، ص 91.

11.75 مليار دولار[1]، الأمر الذي يظهر بوضوح أن هذه الأفعال الإجرامية أصبحت تشكل خطراً جدياً يهدد صناعة المعلوماتية.

157 ـ وقد كفل المشرع الأردني حماية لبرامج الحاسوب من خلال قانون حماية حق المؤلف رقم (22) لسنة 1992. وحتى تكتسب هذه البرامج الحماية المنصوص عليها في قانون حماية حق المؤلف لا بد أن تتمتع بشرط الابتكار حيث تنص المادة (3) من هذا القانون على انه،

"أ ـ تتمتع بالحماية بموجب هذا القانون المصنفات المبتكرة في الآداب والفنون والعلوم أياً كان نوع هذه المصنفات أو أهميتها أو الغرض من إنتاجها.

ب ـ تشمل هذه الحماية المصنفات التي يكون مظهر التعبير عنها الكتابة أو الصوت أو الرسم أو التصوير أو الحركة وبوجه خاص...... برامج الحاسوب بلغة المصدر أو بلغة الآلة."

والجرائم التي قد تقع على برامج الحاسوب وفقاً لهذا القانون هي جريمة تقليد برامج الحاسوب وكذلك جريمة التعامل بالبرامج المقلدة وقد تم النص على هذه الجرائم في المادة (51) من ذات القانون[2].

158 ـ إن سرقة المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر شبكة المعلومات العالمية (الانترنت) ما زالت بحاجة في تشريعاتنا إلى ما يكفل حمايتها من مخاطر سرقتها. وفي ظل غياب النصوص القانونية التي تكفل الحماية للمعلومات من

---

(1) الزيدي، مرجع سابق، ص 32.

(2) تنص المادة 51 من قانون الملكية الفكرية رقم22 لسنة 1992على ما يلي:

"أ ـ يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد عن ثلاث سنوات وبغرامة لا تقل عن الف دينار ولا تزيد على ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين:

1- كل من باشر بغير سند شرعي احد الحقوق المنصوص عليها في المواد(8،9،10،23) من هذا القانون.

2- كل من عرض للبيع او للتداول أو للإيجار مصنفاً مقلداً او نسخاً عنه او إذاعة على الجمهور بأي طريقة كانت أو ادخله إلى المملكة او اخرجه منها مع علمه بانه مقلد.

ب ـ وفي حال تكرار أي جريمة من الجرائم المنصوص عليها في الفقرة (أ) من هذه المادة يحكم على مرتكبها بالحد الأعلى لعقوبة الحبس وبالحد الأعلى للغرامة وللمحكمة في هذه الحالة الحكم بإغلاق المؤسسة التي ارتكبت فيها الجريمة لمدة لا تزيد على سنة أو وقف ترخيصها لمدة معينة أو بصورة نهائية."

مخاطر سرقتها وبناء على ما سبق سنتناول ابتداء ماهية المعلومات ومدى انطباق وصف الأموال عليها في (المطلب الأول)، ثم نحاول البحث بعد ذلك في مدى انطباق أركان جريمة السرقة في قانون العقوبات الأردني على سرقة المعلومات في (المطلب الثاني).

المطلب الأول: ماهية المعلومات ومدى انطباق وصف الأموال عليها

159 ـ نتناول في هذا المطلب تعريف المعلومات وماهيتها في (الفرع الأول)، ثم نحاول الوقوف بعد ذلك على مدى انطباق وصف المال على المعلومات في (الفرع الثاني).

أولاً: ماهية المعلومات

الحديث حول ماهية المعلومات يتطلب الإشارة أولاً إلى تعريف المعلومات ثم بيان الشروط الواجب توافرها في المعلومات حتى تتمتع بالحماية القانونية.

1- تعريف المعلومات:

160 ـ يعرف الأستاذ باركر المعلومات بأنها: (مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال، أو التفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة)[1].

ويعرف البعض الآخر المعلومات أنها: (كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات أو تحليلها أو استقراء دلالاتها أو استنتاج ما يمكن استنتاجه منها وحدها أو متداخلة مع غيرها أو تفسيرها على نحو يثري معرفة متخذي القرار ومساعدتهم على الحكم السديد على الظواهر والمشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية)[2].

(1) مشار له عند، قورة، مرجع سابق، ص93.

(2) شتا، مرجع سابق، ص62.

161 ـ وتعرف البيانات[1] أنها: (المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما). وتسمى العلاقة بين المعلومات والبيانات بالدورة الاسترجاعية للمعلومات، إذ يتم تجميع وتشغيل البيانات والحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة[2].

أما الأستاذ (Catala) فيعرف المعلومة[3] أنها: (رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير).

162 ـ أما في القانون الأردني فقد ورد تعريف للمعلومات في قانون المعاملات الالكترونية المؤقت رقم 85 لسنة 2001، حيث عرف المعلومات أنها: (البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات[4] وبرامج الحاسوب وما شابه ذلك).

وهذا التعريف للمعلومات تعريف فضفاض حيث أن ما ورد من تعداد لصور المعلومات هو تعداد على سبيل المثال لا الحصر.

163 ـ ويتضح من التعريفات السابقة ووفقا لما استقر عليه الفقه أيضا أن المعلومات هي من قبيل الأشياء المعنوية لا المادية وهو الأمر الذي شكل ـ كما سنرى لاحقا ـ عقبة في مجال تطبيق نصوص جريمة السرقة التقليدية على سرقة المعلومات ؛ ذلك أن هذه النصوص تفترض أن محل الاعتداء هو المنقول المادي ومن المسلم به انعدام الكيان المادي والملموس للمعلومات.

---

(1) المصدر السابق، ص 61.

(2) الغريب، مرجع سابق، ص81.

(3) مشار له عند ، الشوا، ثورة المعلومات... مرجع سابق، ص 174.

(4) تعرف قواعد البيانات أنها: (مجموعة من البيانات التي تخص موضوعا معيناً يتم تجميعها وترتيبها وتصنيفها بطريقة مبتكرة أفرزتها تكنولوجيا الحاسوب وتم تخزينها في جهاز الحاسوب بحيث تشكل قاعدة عريضة من البيانات المفيدة التي يمكن استرجاعها والاستفادة منها عند الحاجة إليها) انظر، الحفناوي، مرجع سابق، ص 268.

164 ـ وتجدر الإشارة أخيراً إلى أن المعلومات بصفة عامة تتميز بقابليتها للدمج فقد تضاف معلومة إلى معلومة أخرى لتكونا معاً معلومة جديدة تختلف في قيمتها وأهميتها عما كانت عليه قبل الدمج[1].

2- الشروط الواجب توافرها في المعلومات

165 ـ هناك شروط لا بد أن تتوافر في المعلومة بصفة عامة ـ سواء أكان التعبير عنها يتم من خلال وسيط مادي أم كانت بمعزل عن هذا الوسيط ـ حتى يمكن أن تتمتع بالحماية القانونية وتتجلى هذه الشروط في ما يلي:

أ- أن يتوافر في المعلومة التحديد والابتكار:

166ـ إن المعلومة التي تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية. فالمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون محددة؛ لأن التبليغ الحقيقي يفترض التحديد[2] كما أن المعلومة المحددة هي التي يمكن حصرها في دائرة خاصة بها من الأشخاص.

167 ـ أما فيما يتعلق بالابتكار فإنه ينبغي أن تنصب هذه الصفة على الرسالة التي تحملها المعلومة. فمعلومة غير مبتكرة هي معلومة عامة شائعة ومتاحة للجميع ويمكن للجميع الوصول إليها ولا يمكن نسبتها إلى شخص محدد[3].

---

(1) على سبيل المثال رقم حساب العميل في البنك معلومة على قدر من الأهمية إلا أنه إذا أضفنا إلى هذه المعلومة معلومة أخرى كاسم البنك واسم العميل وحجم الرصيد فان قيمة المعلومة وأهميتها في هذه الحالة تتضاعف وتتطلب قدراً أكبر من الحماية. ولهذا السبب تقوم البنوك بإرسال كل معلومة منفردة عن طريق عمليات اتصال مختلفة فهي على سبيل المثال تقوم بإرسال مجموعة كبيرة من أرقام الحسابات عن طريق عملية اتصال وتقوم بإرسال قيمة الارصدة عن طريق عملية اتصال أخرى. ويتم تجميع المعلومات المختلفة في مركز لمعالجتها وذلك بهدف الحفاظ على سرية هذه المعلومات. انظر قورة، مرجع سابق، ص 96095.

(2) Catala (Pierre), "les Transformations de Droit par L' imformatique" Bensoussan (Alian), linamt de Bellefonds (Xavier), aisl (Herbert) (eds.), Emergences du Droit de L' informateque, 1983, P. 264

مشار له عند، الشوا، ثورة المعلومات... مرجع سابق، ص 175.

(3) المصدر السابق، ص 175. وفي نفس المعنى انظر، محمود، مرجع سابق، ص 155.

ب- أن يتوافر في المعلومة السرية والاستئثار:

168 ـ كلما اتسمت المعلومة بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها هذه المعلومة محدداً بمجموعة معينة من الأشخاص. ودون هذا التحديد لا يمكن أن تكون المعلومة محلاً يعتدى عليه بالسرقة أو النصب أو الإتلاف على سبيل المثال. فالمعلومة غير السرية تكون صالحة للتداول ومن ثم تكون بمنأى عن أي حيازة. وهذا ما ينطبق على المعلومات التي تتعلق بحقيقة معينة كدرجة الحرارة في وقت معين أو تلك المعلومات التي ترد على حوادث معينة كالبراكين والفيضانات فهي تبدو كأنماط قابلة للنقل بسهولة بين كل الأشخاص والوصول إلى المعلومة بسهولة يتعارض والطابع السري لها[1].

قد تستمد المعلومة سريتها من طبيعتها كاكتشاف في أحد المجالات التي تتميز بالسرية. أو قد تستمد سريتها بالنظر لرغبة صاحبها وإرادته أو للسببين معاً، كما هو الحال في الرقم السري لبطاقات الائتمان[2].

169 ـ وتعد خاصية الاستئثار بالمعلومة أمراً ضرورياً لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، وتتوافر للمعلومة صفة الاستئثار إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين ويمكن أن ينبع الاستئثار من سلطة شخص أو جهة ما على المعلومة وعلى التصرف فيها[3].

ثانياً: مدى انطباق وصف المال على المعلومات

170 ـ من المسلم به أن الشق المادي للنظام المعلوماتي والمتمثل في جهاز الحاسوب والمعدات الملحقة به والدعامات والأشرطة المغناطيسية والأقراص بكلٌ أشكالها التي تخزن عليها المعلومات والكابلات وشبكات الربط وغير ذلك، هي مال مادي منقول له

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 176,175 وفي نفس المعنى انظر، قورة. مرجع سابق، ص 109.

(2) انظر، قورة، مرجع سابق، ص 176.

(3) الشوا، ثورة المعلومات... مرجع سابق، ص 176.

كيان خارجي ملموس وبالتالي فإن جريمة السرقة المنصوص عليها في قانون العقوبات يمكن أن تقع على هذا الجانب من مكونات النظام المعلوماتي.

أما فيما يتعلق بالشق المعنوي للنظام المعلوماتي والمتمثل في المعلومات والبيانات والبرامج وغير ذلك فان التساؤل يثور في ما إذا كان بالإمكان انطباق وصف الأموال عليها بالرغم من طبيعتها اللامادية (المعنوية).

171 ـ ابتداء نشير إلى أن الاتجاه الذي كان سائدا في تحديد مدى انطباق وصف المال على الأشياء كان يعتمد على صفة المادية في الأشياء لاعتبارها مالاً. فقد كان هذا الاتجاه يعرف المال أنه: "كل شيء يمكن حيازته مادياً"[1]. وبالتالي فالأشياء المعنوية لا تتمتع من وجهة نظرهم بصفة المال، فقد كان ينظر إليها باعتبارها إما عديمة القيمة أو ذات قيمة منخفضة.

172 ـ إلا أن التطورات التي حدثت في العقود القليلة الماضية التي ما زالت مستمرة للآن في مجال تكنولوجيا المعلومات جعلت المعلومات تنتشر بصورة كبيرة في مجال المعاملات المختلفة مما أدى في بعض الأحيان إلى ارتفاع قيمتها عن قيمة الأموال المادية، وخاصة مع استخدام الحاسبات في مجال التجارة إبان الحرب العالمية الثانية بعد أن كانت سراً حربياً مقصوراً على الخاصة لسنوات طويلة، وبالكشف عنها بزغ عقد زمني جديد أطلق عليه عقد انفجار المعلومات باعتباره العقد الذي شهد الغزو الموسع للحاسبات بما لها من قدرات هائلة على التخزين والاسترجاع. ولم يقف الأمر عند هذا الحد بل تم التفاعل بين عملاقين وهما: علم المعلوماتية وعلم الاتصالات مما أسفر عن تحول العالم إلى وحدة سكنية واحدة[2]، وأصبحت المعلومات تنساب بسهولة ويسر بين الأفراد وأصبحت تشكل قوة حقيقية لمن يمتلكها.

---

(1) المناعسة وآخرون، مرجع سابق، ص114.

(2) لطفي، محمد حسام. الجرائم التي تقع على الحاسبات أو بواسطتها. ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 448 ـ 490.

173 ـ وهذا التطور أدى بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال، حيث تم اللجوء إلى معيار آخر ألا وهو معيار القيمة الاقتصادية للشيء[1]. حيث يعتبر الشيء مالاً ليس بالنظر إلى ماله من كيان مادي ملموس وإنما بالنظر إلى قيمته الاقتصادية. وهذا ما ذهب إليه الأستاذ (Carbonnier) حيث قال: (إنه من الواضح أن أي قانون يرفض أن يرى قيمه في شيء له أهمية اقتصادية سيبقى حتما بمعزل عن الحقيقة)[2].

ووفقا لهذا الاتجاه يمكن إسباغ صفة المال على المكونات المعنوية للنظام المعلوماتي على أساس ما تتمتع به من قيمة اقتصادية.

174 ـ أما فيما يتعلق بتحديد المقصود بالأموال في القانون الأردني، فالمشرع الجزائي الأردني لم يحدد المقصود بالمال وبالتالي كان لا بد من الرجوع إلى القانون المدني، والذي نص في المادة (53) منه على أن المال هو: (كل عين أو حق له قيمة مادية في التعامل).

ونصت المادة (54) كذلك على أن (كل شيء يمكن حيازته مادياً أو معنوياً والانتفاع به انتفاعاً مشروعاً ولا يخرج عن التعامل بطبيعته أو بحكم القانون يصح أن يكون محلاً للحقوق المالية).

ويلاحظ أن المشرع في المادة (54) استخدم تعبير (كل شيء)، وهذه الكلمة جاءت مطلقة ولا ترتبط حتماً بكلمة مادي وكما هو معروف فالمطلق يبقى على إطلاقه ما لم يرد نص يقيده[3].

175 ـ كذلك بينت المادة (54) الشروط الواجب توافرها في الشيء حتى يصلح محلاً للحقوق المالية. وهذه الشروط هي إمكانية الانتفاع بهذا الشيء انتفاعاً مشروعاً لا يخرج عن التعامل بطبيعته أو بحكم القانون وإمكانية حيازته مادياً أو معنوياً[4].

---

(1) عفيفي، مرجع سابق، ص112.

(2) مشار له عند، الشوا، ثورة المعلومات... مرجع سابق، ص 184.

(3) المناعسة وآخرون، مرجع سابق، ص 116.

(4) هذا ما أكدت عليه أيضا المذكرة الإيضاحية للقانون المدني الأردني في سياق شرحها للمادتين 45,53 المتعلقتين بتعريف المال، حيث أوضحت أن الشيء يكون مالاً إذا توافر فيه شرطان هما: الحيازة وإمكانية الانتفاع المادي به. انظر، السعيد، جرائم الكمبيوتر... مرجع سابق، ص 354.

176 ـ بالنسبة للشرط الأول وهو إمكانية الانتفاع بالشيء، فالمعلومات يمكن الانتفاع بها وتحقيق عوائد مالية ضخمة من ورائها خاصة في وقتنا الحالي. والمعلومات لا تخرج كذلك عن التعامل بطبيعتها أو بحكم القانون، حيث أن الشيء يخرج عن التعامل بطبيعته إذا كان من الأشياء التي لا يستطيع أحد الاستئثار بها كمياه البحار وأشعة الشمس، ويخرج الشيء عن التعامل بحكم القانون متى حظر القانون التعامل به بصفة مطلقة كالإنسان حياً أو ميتاً أو بصفة نسبية كالمخدرات[1].

177 ـ أما بالنسبة لشرط الحيازة، فالمشرع أشار في المادة (45) إلى أن حيازة الشيء يستوى فيها أن تكون حيازة مادية أو حيازة معنوية.

وفي سياق شرح المذكرة الإيضاحية للقانون المدني الأردني للحيازة المادية والحيازة المعنوية أوضحت المذكرة أن الحيازة تكون مادية إذا كان الشيء المحتاز ماديا، فحيازة الأشياء المادية تكون بحيازتها مادياً، في حين تكون الحيازة معنوية إذا كان الشيء المحتاز معنوياً، فحيازة الأشياء المعنوية تكون بحيازتها معنوياً وحيازتها معنوياً تكون بصدورها عن صاحبها ونسبتها إليه.

واستناداً إلى ما سبق يمكن القول إن الشق المعنوي للنظام المعلوماتي يعتبر من قبيل الأموال المعنوية التي يمكن الانتفاع بها واستغلالها وكذلك يمكن حيازتها معنويا.

المطلب الثاني: مدى انطباق وصف السرقة في قانون العقوبات الأردني على سرقة المعلومات

178 ـ السرقة هي الجريمة الأولى المنصوص عليها في قانون العقوبات الأردني تحت عنوان الجرائم الواقعة على الأموال، وقد وردت النصوص الخاصة بها وبالجرائم الملحقة بها في الفصل الأول من الباب الحادي عشر من الكتاب الثاني في المواد (339 ـ 416) من قانون العقوبات.

---

(1) نجم، محمد وصالح، نائل، قانون العقوبات الأردني (القسم الخاص)، بدون ناشر، 1999، ص32.

179 ـ عرفت المادة (399) من ذات القانون السرقة على أنها: (أخذ مال الغير المنقول دون رضاه). ووفقا لنص هذه المادة فإن عناصر جريمة السرقة وأركانها تتمثل في:

1. الركن المادي وهو فعل الأخذ.
2. محل الجريمة وهو المال المنقول المملوك للغير.
3. الركن المعنوي والقائم على القصد العام المتمثل في عنصري العلم والإرادة، والقصد الخاص والمتمثل في نية التملك.

180 ـ وكما هو معروف فإن قيام جريمة السرقة يستلزم توافر هذه الأركان مجتمعة، فإذا تخلف أحدها انتفت الجريمة. ولا توجد مشكلة في حال سرقة الدعامات المادية ذات الكيان المادي الملموس كالإسطوانات المدمجة أو الأشرطة الممغنطة وغير ذلك من أدوات تخزين المعلومات المستخدمة في بيئة الحاسوب، إذ أننا نكون هنا بصدد سرقة مال مادي منقول تمت عملية تبديل حيازته أي إخراجه من حيازة مالكه أو حائزه الشرعي وإدخاله في حيازة الجاني، أي أن السرقة بمفهومها الوارد في المادة (399) تنطبق على هذه الحالة.

181 ـ ولكن المشكلة تثور في الحالة التي يقوم بها الفاعل بالحصول على المعلومات المخزنة داخل النظام المعلوماتي دون وجه حق، كما هو الحال إذا قام الفاعل بالتزود بدعامة مادية خالية يملكها وقام بتسجيل ما يريد من المعلومات الخاصة بالغير عليها، فهل يمكن القول بتوافر أركان جريمة السرقة الواردة في المادة (399) من قانون العقوبات الأردني على هذه الحالة.

182 ـ لا بد أن نشير ابتداءً إلى أن المشرع الأردني قد وضح مضمون فعل الأخذ المكون للركن المادي لجريمة السرقة في الفقرة الثانية من المادة (399) حيث جاء فيها " وتعني عبارة (أخذ المال): "إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلاً بغير منقول فبفصله عنة فصلا تاما ونقله".

وحتى تكون عناصر فعل الأخذ قد تحققت كما حددتها المادة 2/399 من قانون العقوبات الأردني لا بد من توافر عنصرين هما[1]:

1. إخراج المال محل جريمة السرقة من حيازة المجني عليه.
2. إدخال المال في حيازة الجاني أو شخص ليس له حق في ذلك.

ومن خلال هذين العنصرين نلاحظ أن المشرع الجزائي الأردني قد تبنى مبدأ تحريك المال المسروق برفعه من مكانه، حيث يؤدي هذا التحريك إلى إخراج المال من حيازة المجني عليه وإدخاله في حيازة شخص آخر ليس له حق فيه[2]، وهو ما يعرف بتبديل الحيازة.

183 ـ في ظل هذا التحديد نجد أن مفهوم السرقة يتضمن نقلاً من حيازة إلى حيازة أخرى، ومن يقوم بسرقة المعلومات بشكل مستقل عن الدعامة المادية لم يخرج المعلومات من حيازة مالكها[3] حيث لم يترتب على سلوك الفاعل هنا حرمان صاحبها منها، وان أدى سلوكه إلى التأثير في قيمة هذه المعلومات من الناحية الاقتصادية. وبالتالي يتضح لنا أن مفهوم فعل الأخذ المشكل للركن المادي في جريمة السرقة غير متوافر في هذه الحالة.

184 ـ أما بالنسبة لموضوع أو محل جريمة السرقة فهو المال المنقول المملوك للغير. والعلة من وراء اشتراط أن يكون موضوع السرقة مالاً، أن السرقة جريمة اعتداء على الملكية ولا يصلح محلاً للملكية إلا شيء له صفة المال وفقاً للقانون[4].

والمال الذي يصلح محلاً لجريمة السرقة هو المال المادي المنقول والذي له كيان خارجي ويشغل حيزاً في محيطنا ويمكن لمسه. وبالتالي فإن المعلومات لا تصلح محلاً لجريمة السرقة لكونها مالاً معنوياً يتجرد من الصفة المادية.

---

(1) نجم وصالح، مرجع سابق، ص 299. وانظر كذلك، دلالعة، سامر، الحماية الجنائية لبرامج الحاسوب، بحث مقدم لمؤتمر القانون والحاسوب، جامعة اليرموك، اربد، من12 ـ 14 تموز، ص35.

(2) المصدر السابق، ص299.

(3) قضت محكمة التمييز الأردنية في إحدى قراراتها ان: (مجرد الاطلاع على أسئلة الامتحانات وإفشائها لا يشكل سرقة مال بالمعنى القانوني) تمييز جزاء 81/93. مجلة نقابة المحامين، تشرين الأول 1981، س29، ص1776.

(4) حسني، محمود نجيب، جرائم الاعتداء على الأموال، ط1، بدون ناشر، 1969، ص34.

فالمال المادي الملموس هو الذي يتقبل السلطات المادية التي تنطوي عليها الملكية والحيازة، وكذلك فإن الحيازة التي تنالها السرقة بالاعتداء يراد بها الحيازة المادية التي تتمثل في سيطرة الحائز على الشيء أو المال ومباشرته عليه سلطات مادية[1].

185 ـ ومما يؤكد أيضا أن محل السرقة هو المال المنقول المادي أن المشرع بتحديده لفعل الأخذ أشار إلى أنه يتضمن رفع المال ونقله من مكانه، أي أن مضمون فعل الأخذ يتطلب من الفاعل القيام بتصرف مادي يتضمن تحريك الشيء من مكانه وهذا التحريك لا يتصور أن يتم إلا على الأموال المادية التي لها كيان مادي محسوس. وبالتالي فإن الأشياء أو الأموال التي لا تتمتع بالصفة المادية تخرج من إطار جريمة السرقة كما حددتها المادة (399) من قانون العقوبات الأردني، كالمعلومات والأفكار والحقوق والمنافع إذ أنها أشياء متجردة من الطبيعة المادية ولا يتصور ممارسة السلطات المادية عليها.

186 ـ إلا أن البعض[2] يرى أن التطور لتكنولوجي الموجود أو المحتمل وجوده فيما بعد يفرض علينا أن نعتد بفكرة الكيان المادي للشيء. فالبرنامج أو المعلومة ـ وفقاً لهذا الرأي ـ لا يمكن أن يكونا شيئاً ملموساً ومحسوساً لكن لهما كيان مادي يمكن رؤيته على الشاشة مترجم إلى أفكار، وأن المعلومات المتنقلة عبر الأسلاك على شكل نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل ومولد صادرة عنه يمكن سرقته وبالتالي لها كيان مادي. كما أنه يمكن الاستحواذ على هذه البرامج والمعلومات عن طريق تشغيلها أي وضعها في جهاز الحاسوب واستعمال التكنيك اللازم للتشغيل عن طريق استخدام كلمة السر.

187 ـ إلا أننا نرى انه لا يمكن التسليم بفكرة الكيان المادي للمعلومات، فهي ذات طبيعة معنوية ـ كما سبق وبينا ـ ولا تشغل حيزاً في المحيط الخارجي ولا يمكن القول بتمتعها بالكيان المادي لمجرد أن التطور التكنولوجي يفرض علينا ذلك، بل لا بد من وضع الأحكام والنصوص القانونية التي تتناسب وطبيعتها الخاصة.

---

(1) المصدر السابق، ص34.

(2) قشقوش، مرجع سابق، ص63، 62.

188 ـ إلا أنه وفي ظل توسع المشرع الجزائي الأردني في مدلول لفظ المال ليشمل القوى المحرزة وذلك في الفقرة الثالثة من المادة (399)، فهل يمكن القول بانطباق وصف الطاقة أو القوى على المعلومات؟

ابتداء نشير إلى أن القوى المحرزة هي طاقات تتولد تلقائياً أو عن طريق عمل الإنسان الذي يستطيع السيطرة عليها وتسخيرها في متطلبات حياته، أي يستطيع حيازتها ومباشرة سلطات الحيازة عليها، وتعبير القوى المحرزة ينصرف في المقام الأول إلى الكهرباء[1].

189 ـ أما فيما يتعلق باعتبار المعلومات من قبيل القوى المحرزة وقياس سرقتها على سرقة الكهرباء، فقد ذهب البعض[2] إلى أن المشرع الأردني ـ وإن كان قد وسع من مدلول المال على نحو أصبح يشمل معه القوى المحرزة ـ إلا أنه لا يمكن القول بانطباق وصف الطاقة أو القوة على المعلومات.

190 ـ بينما ذهب البعض[3] الآخر إلى أن البيانات والمعلومات التي تخضع لسيطرة من يبتكرها ويستطيع الانتفاع بها وتصلح للخروج من حيازته والدخول في حيازة أخرى، ولها مقابل مادي بالبيع والشراء هي مما يمكن أن ينطبق عليه وصف الطاقة أو القوى، وبالتالي يمكن أن يقع عليها فعل الأخذ والمشكل أحد عناصر الركن المادي لجريمة السرقة، مثلها مثل الكهرباء.

191 ـ إلا أننا نؤيد الاتجاه الأول الذي يرى عدم إمكانية إسباغ وصف الطاقة أو القوى على المعلومات، إذ أن المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكات المحلية أو العامة هي عبارة عن نبضات الكترونية ولا يمكن اعتبارها طاقة أو قوة كما هو الحال بالتيار الكهربائي. كما أن اعتبار المعلومات من قبيل القوى المحرزة هو توسع في تفسير الفقرة الثالثة من المادة (399) من قانون العقوبات الأردني

---

(1) حسني، مرجع سابق، ص 35 . ويرى د.محمود حسني بأن القوى المحرزة تشمل كذلك القوى النووية.

(2) السعيد، جرائم الكمبيوتر... مرجع سابق، ص 353.

(3) الشوابكة، محمد أمين. جرائم الحاسوب والانترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004، ص141. وتذهب د.هدى قشقوش كذلك إلى إمكانية قياس سرقة المعلومات على سرقة الكهرباء. انظر في ذلك، قشقوش، مرجع سابق، ص 63،64.

وهو الأمر الذي يتنافى مع المبدأ الجوهري في القانون الجنائي وهو مبدأ شرعية الجريمة والعقوبة وعدم جواز التوسع في تفسير النصوص الجزائية.

192 ـ كما أنه لا يمكن قياس سرقة المعلومات على سرقة التيار الكهربائي فقدْ استقر الفقه والقضاء على اعتبار الكهرباء من قبيل الأشياء المادية. فالكهرباء قوة وطاقة تخضع لسيطرة من يولدها ويستطيع التحكم بها واستعمالها فيما يبتغي من أغراض وتمكين غيره من استعمالها ويعني ذلك أنها تصلح موضوعاً للملكية والحيازة[1]، أي أنها تصلح محلاً لجريمة السرقة.

كما أن الكهرباء صالحة للنقل من موضع إلى آخر وصالحة بالتالي للخروج نهائيا من حيازة صاحبها والدخول في حيازة شخص آخر ليس له الحق فيها[2]، مما يعني إمكانية تحقق فعل الأخذ والمشكل للركن المادي في جريمة السرقة كما بينه المشرع في الفقرة الثانية من المادة (399).

193 ـ كما تجدر الإشارة إلى أن الكهرباء بطبيعتها قابلة للقياس حيث يمكن تحديدها من حيث الكم بتحديد مصدرها والمسافة التي تقطعها ومكان وصولها بطريقة علمية، أي على وجه الدقة، كما أنها لا توجد في عدة أمكنة في وقت واحد. في حين أن المعلومات ـ وإن كان يمكن تحديدها من حيث الكم ـ إلا أنه لا يمكن بأي حال من الأحوال أن ينجم عن هذا التحديد قياس دقيق لها كما هو الحال فيما يتعلق بالكهرباء، بحيث يمكن احتساب المقدار الذي تم سرقته منها على وجه الدقة. كما أن المعلومة الواحدة يمكن تسجيلها على أكثر من وسيط مادي مختلف بحيث يوجد عدد لا حصر له من المعلومة الواحدة، وهو ما يختلف تماما عن الكهرباء[3].

194 ـ بناء على ما تقدم نجد أن تصور سرقة المعلومات أمر غير ممكن في قانون العقوبات الأردني؛ وذلك لتخلف أهم أركان جريمة السرقة كما حددها المشرع في

---

(1) حسني، مرجع سابق، ص36.

(2) المصدر السابق، ص37.

(3) قورة، مرجع سابق، ص160، 161. وتذهب د ـ واثبة السعدي كذلك إلى عدم إلحاق المعلومات وبرامج الحاسوب بالقوى المحرزة. انظر، السعدي، واثبة، الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب، المنعقد في جامعة اليرموك، اربد من 12 ـ 14 تموز (2004)، ص 26.

المادة (399). فلا يمكن القول بوقوع الأخذ وهو الفعل المكون للركن المادي لجريمة السرقة على سرقة المعلومات وكذلك فإن المعلومات لا تشكل محلاً صالحاً لوقوع جريمة السرقة عليها. وبالتالي وإعمالاً لمبدأ شرعية الجريمة والعقوبة ولتجنب القياس والتوسع في تفسير النصوص الجزائية نجد أن المشرع الجزائي الأردني لا بد أن يتدخل لتجريم هذا الفعل بشكل يراعي الطبيعة الخاصة للمعلومات.

المبحث الثاني
الاستعمال غير المصرح به للنظام المعلوماتي

195 ـ إن الانتشار الواسع للحواسيب وللشبكات المعلوماتية التي تربط بينها والاعتماد الكبير من قبل القطاعين العام والخاص على الأنظمة المعلوماتية في سبيل انجاز الأعمال المختلفة، اوجد معه تساؤلاً حول مدى مشروعية الاستعمال غير المصرح به لهذه الأنظمة من قبل بعض الأفراد والتكييف القانوني لهذا الفعل.

196 ـ وهناك عدة مصطلحات تستخدم للدلالة على هذا السلوك حيث يطلق عليه البعض: "سرقة منفعة الحاسوب[1] أو تشغيل الحاسوب دون مقابل[2] أو سرقة الخدمات التي يقدمها الحاسوب".

197 ـ ويمكن تعريف الاستعمال غير المصرح به للنظام المعلوماتي على أنه: (كل استعمال للوظيفة التي يؤديها الحاسوب خلال فترة زمنية دون أن يكون مصرحاً بذلك الفاعل، و بمعنى آخر هو كل استخدام للحاسوب ولنظامه للاستفادة من الخدمات التي يقدمها دون أن يكون للشخص الذي يمارس هذا الاستخدام الحق في ذلك) [3].

وللوقوف على هذا السلوك غير المشروع أتناول ابتداء الآراء الفقهية المتضاربة حول التكييف القانوني لهذا السلوك في (المطلب الأول)، ثم أعرض بعد ذلك مدى توافر الحماية الجنائية للنظام المعلوماتي من هذا الاستخدام غير المصرح به في قانون العقوبات الأردني في (المطلب الثاني).

المطلب الأول: التكييف القانوني لاستعمال النظام المعلوماتي

198 ـ لا بد أن نشير ابتداء إلى أن الغالبية العظمى من أفعال الاستعمال غير المصرح به يقوم بها العاملون والموظفون في القطاعين العام والخاص الذين يكون لهم

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 220.

(2) الصغير، مرجع سابق، ص 31.

(3) قورة، مرجع سابق، ص 392.

الحق في استخدام النظام المعلوماتي لمدة أو لغرض محدد. وفي الواقع فان هذا السلوك شائع ومنتشر بين أوساط العاملين في المؤسسات المختلفة، وذلك لعدم وجود الشعور بعدم أخلاقية أو مشروعية هذا الفعل[1] بين هؤلاء المستخدمين.

199 ـ وبالرغم من أن الاستعمال غير المصرح به للنظام المعلوماتي لا يسبب خسائر اقتصادية كبيرة مقارنة بالجرائم المعلوماتية الأخرى، إلا انه يمس مصالح جديرة بالحماية، كالمصالح الاقتصادية للمؤسسة التي قد يصيبها كثير من الضرر خاصة في الحالات التي تلتزم فيها الشركة أو المؤسسة بتسديد قيمة الوقت الفعلي لهذا الاستخدام.

وكذلك لا بد من حماية النظام المعلوماتي ذاته من هذا الاستعمال غير المصرح به حتى يستطيع القيام بوظائفه على أكمل وجه، إذ قد يتسبب هذا الاستعمال في أن تفقد المؤسسة خدماتها أو عملائها بسبب إعاقة النظام عن أداء عمله وزيادة تحميله وهو ما يؤدي إلى تعطيله في كثير من الحالات[2].

200 ـ تتفاوت استعمالات النظام المعلوماتي بين مجرد قيام العامل أو الموظف باستخدام النظام للقيام ببعض الألعاب في أوقات الفراغ أو لنسخ الألعاب أو لتحرير بطاقات لأعمال الخير، أي قد يقوم باستخدامه لغايات تخلو من أي هدف مادي أو إجرامي، وقد يتم استخدام النظام لانجاز أعمال خاصة بهذا العامل إما لتحقيق غايات تجارية أو إجرامية أو غير ذلك.

(1) استطلاع للرأي قامت به المؤسسة العامة لشركات التأمين ضد الحريق والمخاطر الأخرى في فرنسا (APSAIRD)، وكان السؤال المطروح على العاملين في المؤسسة كالآتي: هل من الممكن ان تستخدموا الأنظمة المعلوماتية داخل المؤسسات التي تعملون بها لأغراض شخصية ؟؟ وكانت نتيجة الاستطلاع ان اجاب 23٪ فقط النفي، لأن ذلك يشكل عملاً غير مشروع، في حين ان 77٪ اجاب بالإيجاب على اعتبار أن ذلك يعد عملاً مألوفاً من بينهم 19٪ قاموا فعلاً باستخدام الحاسوب لأغراض شخصية.

Estimation des Pertes dues a' L' informatique. Le Monde Informatique, 6 juin 1988, P.29.

مشار اليه عند، قورة، مرجع سابق، ص396.

(2) المصدر السابق، ص388.

201 ـ والاستعمال غير المصرح به يمارس بشكل أساسي على الخدمات التي يقدمها النظام المعلوماتي، وهذه الخدمات تشمل معالجة وتخزين وإرسال المعلومات والبيانات وكذلك استخدام الشبكات المعلوماتية المحلية أو العامة.

202 ـ أما فيما يتعلق بالوصف أو التكييف القانوني الذي يمكن إضفائه على فعل الاستعمال غير المصرح به للنظام المعلوماتي فقد تضاربت الآراء الفقهية في هذا المجال، وكان هناك عدة اتجاهات:

الاتجاه الأول:

203 ـ ذهب هذا الاتجاه إلى تطبيق النصوص الخاصة بجريمة السرقة على هذا الفعل.إلا أنه من غير الممكن إضفاء وصف السرقة على الاستعمال غير المصرح به، ذلك أن الفاعل هنا لا يقوم بالاستيلاء على مال مادي منقول، كما انه لا يخرج شيئاً من حيازة مالكه ويدخله في حيازته، بل إن القصد الجرمي الخاص والمطلوب توافره في جريمة السرقة وهو نية التملك غير متوافر، حيث إن فعل الجاني يقتصر على استعمال الخدمات المعلوماتية.

204 ـ في الاتجاه ذاته يرى البعض أن الفعل يشكل سرقة للتيار الكهربائي أو الطاقة. وقد تم انتقاد هذا الرأي استناداً إلى أنه لا يوجد في هذه الحالة استخدام لموصل مخصص لسحب الطاقة بانتظام[1]، كما أنه في حال استخدام النظام المعلوماتي عن طريق طرفية بعيدة (Remote Terminal) تتصل بالنظام يكون الفاعل في هذه الحالة قد تسبب في استخدام النيار الكهربائي لكنه لم يستخدمه مباشرة بنفسه[2].

الاتجاه الثاني:

205 ـ وفقا لهذا الاتجاه فإن استخدام الفاعل كلمة السر أو الشيفرة الخاصة للدخول إلى النظام المعلوماتي يعتبر بمثابة انتحال اسم كاذب أو صفة غير صحيحة[3] وهذا يشكل بدوره جريمة احتيال.

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص222.

(2) قورة، مرجع سابق، ص403.

(3) هذا ما ذهب إليه الفقيه R.Gassin مشار له عند، الشوا، ثورة المعلومات... مرجع سابق، ص223.

206 ـ لكن من الصعب قبول هذا التكييف خاصة في الحالة التي يقوم بها العاملون أو الموظفون الذين يكون من المصرح لهم الدخول إلى النظام المعلوماتي لأداء غرض معين ولمدة محددة ـ ويعرفون بالتالي كلمة السر أو الشيفرة الخاصة للدخول إلى النظام - إلا أنهم يستخدمونه لأغراض شخصية أو تجارية أو غير ذلك، حيث لا يوجد هنا استخدام لطرق احتيالية.

الاتجاه الثالث:

207 ـ يذهب أصحاب هذا الاتجاه[1] إلى تطبيق النصوص المتعلقة بجريمة إساءة الائتمان على الاستعمال غير المصرح به للنظام المعلوماتي وذلك في حالة أن كان جهاز الحاسوب وملحقاته قد سلم إلى المستخدم بموجب عقد من عقود الأمانة.

أما في حالة قيام الفاعل بهذا الاستعمال غير المصرح به دون وجود عقد من عقود الأمانة فلا يقع هذا الفعل تحت أي وصف جنائي، حيث لا يوجد هناك انتهاك لأي علاقة تعاقدية وفقا لهذا الاتجاه.

المطلب الثاني: الحماية الجنائية للنظام المعلوماتي من الاستعمال غير المصرح به في قانون العقوبات الأردني

208 ـ لا بد من توفير الحماية القانونية الكافية للنظام المعلوماتي من الاستعمال غير المصرح به لهذا النظام، خاصة أن هذا السلوك يمارس على نطاق واسع. ويثار التساؤل بالتالي حول النص القانوني الذي يمكن تطبيقه في هذا الصدد.

209 ـ باستعراضنا لنصوص قانون العقوبات الأردني نجد أن المشرع الجزائي في الفصل الأول من باب الجرائم الواقعة على الأموال وضع عدداً من النصوص القانونية التي تضمنت طائفة من الجرائم على صلة وثيقة بالسرقة إن كان لا يتوافر فيها كلّ عناصر جريمة السرقة، إلا أن هناك عناصر مشتركة بين السرقة وهذه الجرائم. وقد

(1) A – Bertrand, le Vol de temps machine peut – ilertre qualifie de Vol ? Expertises no.81,1986,P.31.

مشار له عند الشوا، ثورة المعلومات...، مرجع سابق، ص223.

اتفق الفقهاء على إطلاق اصطلاح (الجرائم الملحقة بالسرقة) على هذه الطائفة من الجرائم[1]. ويندرج ضمن هذه الطائفة من الجرائم جريمة استعمال أشياء الغير دون وجه حق التي نصت عليها المادة (416) من قانون العقوبات الأردني، حيث جاء فيها: (كل من استعمل دون حق شيئاً يخص غيره بصورة تلحق به ضرراً دون أن يكون قاصداً اختلاس ذلك الشيء، عوقب بالحبس حتى ستة أشهر وبالغرامة حتى عشرين ديناراً أو بإحدى هاتين العقوبتين).

وفي هذه الجريمة لا تكون نية الفاعل متجهة إلى تملك الشيء الذي حازه لكن تكون نيته متجهة إلى استعمال ذلك الشيء دون الحصول على موافقة مالكه أو حائزه القانوني وبعد ذلك إعادته له.

210 ـ والتساؤل الذي يثار في هذا الصدد أنه إذا كان الاستعمال غير المصرح به للنظام المعلوماتي يقتصر على استخدام الخدمات المعلوماتية التي يقدمها النظام، فما هي إمكانية تطبيق نص المادة (416) من قانون العقوبات الأردني على هذا السلوك؟

بالتمعن في نص المادة (416) نجد أن قيام جريمة استعمال أشياء الغير دون وجه حق يتطلب توافر ثلاثة أركان هي: محل أو موضوع الجريمة والركن المادي والركن المعنوي.

211 ـ فيما يتعلق بموضوع الجريمة يتمثل في المال المملوك للغير، وبناء على الصلة بين جريمة استعمال أشياء الغير دون حق وبين جريمة السرقة لا بد من توافر سائر الشروط المطلوب توافرها في موضوع السرقة، إذ يتعين أن يكون المال ذا طبيعة مادية وأن يكون منقولاً وفي حيازة غير المدعى عليه. فتطلب أن يكون المال ذا طبيعة مادية يفسره أن الاستعمال باعتباره حقاً عينياً أو عنصراً لحق الملكية لا يرد إلا على شيء يتمتع بطبيعة مادية. كما أن هذا المال لا بدّ أن يكون مملوكاً لغير المدعى عليه (الفاعل) لأنه إذا كان مملوكاً له ففعله يكون صورة لإحدى السلطات المتفرعة عن حق ملكيته[2].

(1) نجم وصالح، مرجع سابق، ص 411.

(2) حسني، مرجع سابق، ص 202.

212 ـ أما الركن المادي في هذه الجريمة فيتمثل في فعل الاستعمال الذي يجب أن يتم دون حق بشكل من شأنه أن يلحق بالمجني عليه ضرراً.

213 ـ يقصد بالاستعمال فعل يستخدم به الشيء في أداء خدمة للمدعى عليه أو غيره. ويفترض الاستعمال فعلاً يخرج به الفاعل الشيء من حيازة المجني عليه ويدخله بعد ذلك في حيازته ليستعمله؛ ذلك أن هذه الجريمة تنطوي على المساس بالحيازة أيضا، وبالتالي إذا استطاع الشخص أن يستعمل الشيء المملوك لغيره دون أن يخرجه من حيازته فهو لا يُعد مرتكباً لهذه الجريمة[1].

214 ـ وتجدر الإشارة كذلك إلى أنه لا يعد مرتكباً لهذه الجريمة من كان الشيء في حيازته بصورة مشروعة إلا أنه استعمله على غير الوجه المصرح له به أو بعد انقضاء المدة التي كان مصرحاً له بالاستعمال خلالها[2].

ويطلب المشرع أن يكون هذا الاستعمال دون وجه حق، ففي حال كان الاستعمال بتصريح من المالك أو من صاحب الحق بالاستعمال إذا كان ممن يدخل في سلطته التصريح لغيره بذلك[3]، فلا تقوم جريمة استعمال أشياء الغير دون حق.

215 ـ حتى يكتمل الركن المادي لهذه الجريمة لا بد أن يكون هناك ضرر قد لحق بالشيء المستعمل، فإذا انتفى الضرر انتفت الجريمة.

216 ـ وأخيراً حيث أن جريمة استعمال أشياء الغير دون حق جريمة مقصودة فلا بد من توافر الركن المعنوي المتمثل في القصد الجرمي العام الذي يتألف من عنصري العلم والإرادة. علم الجاني أنه سيستعمل أشياء مملوكة للغير دون رضاه ودون وجه حق، وكذلك اتجاه إرادته إلى إتيان هذا الفعل.

217 ـ باستعراضنا لأركان جريمة استعمال أشياء الغير دون وجه حق نجد أننا أمام نص تقليدي، يتطلب وجود شيء أو مال مادي حتى تقع عليه هذه الجريمة، ومن

---

(1) المصدر السابق، ص203. وفي نفس المعنى انظر، نجم وصالح، مرجع سابق، ص432 وكذلك، العاني، عادل، جرائم الاعتداء على الأموال في قانون العقوبات الأردني، ط1، دار الثقافة للنشر و التوزيع، عمان، 1995، ص138.

(2) حسني، مرجع سابق، ص 203.

(3) العاني، مرجع سابق، ص 139، 138.

المسلم بـه أن الخـدمات المعلوماتيـة لا تتمتـع بكيـان مـادي ملمـوس، كمـا أن فعـل الاستعمال في هذه الجريمة ـ وكما اتفق الفقه ـ يفترض فعلا يخرج به الفاعل الشيء من حيازة المجني عليه ويدخله في حيازته ليستعمله، وهو الأمر الذي لا يتحقق في حالة الاستعمال غير المصرح به للنظام المعلوماتي. وبالتالي لا بد من أن يتدخل المشرع الجزائي الأردني ليحمي النظام المعلوماتي من الاستخدام غير المصرح به الذي قد يلحق ضرراً بالقطاعين العام أو الخاص معاً.

218 ـ أدركت بعض الدول ـ خاصة المتقدمة منها في مجال الاعتماد على الأنظمة المعلوماتية في إنجاز أعمالها ـ عجز النصوص التقليدية عن معالجة هذه الجريمة والتعامل معها، فأفردت لها نصوصاً خاصة.

219 ـ في الولايات المتحدة الأمريكية هناك تجريم للاستعمال غير المصرح به للنظام المعلوماتي في معظم الولايات، ونذكر على سبيل المثال القانون الخاص بجرائم الحاسبات في ولاية فيرجينيا الصادر عام 1986 حيث جاء في النص الذي يجرم هذا السلوك ما يلي:[1] (كل من يستخدم عمداً وبسوء نية حاسباً آليا أو شبكة للحاسبات الآلية بغرض الحصول على الخدمات التي يقدمها الحاسوب أو الشبكة دون أن يكون مصرحاً له بذلك يعد مرتكباً لجريمة سرقة خدمات الحاسوب).

أما على المستوى الفيدرالي في الولايات المتحدة الأمريكية، فلا يحظر الاستعمال غير المصرح به للنظام المعلوماتي إلا إذا ترتب عليه إعاقة الاستخدام المسموح به للحاسوب ونظامه.

220 ـ عدّل المشرع الكندي كذلك من قانون العقوبات حيث أضاف نصاً يجرم الاستعمال غير المصرح به، حيث يعد جريمة وفقاً لهذا النص:[2] (الحصول بطريق

---

(1)Kutz (Robin K), Copmute Crime in Virginia: Acretical Examination of the Criminal Offences in the Virginia.Copmuter Crimes Act, W.M.L.Rev, 1986,vol – 27,P.783.
مشار له عند، قورة، مرجع سابق، ص 423,422.

(2) هذا ما أشارت إليه الفقرة الثانية من المادة 342 من قانون العقوبات الكندي لعام 1985 مشار له عند، قورة، مرجع سابق، ص428.

مباشر أو غير مباشر على أي من الخدمات التي يقدمها الحاسوب متى تم ذلك بسوء نية ودون وجه حق، أو كان الاستعمال بغية ارتكاب جريمة أخرى).

221 ـ كذلك الحال بالنسبة للمشرع الاسترالي الذي نص على تجريم هذا السلوك بإضافة المادة 115 إلى قانون العقوبات الاسترالي لعام 1985.

222 ـ أما في فرنسا فيرى البعض[1] إمكانية تطبيق النص الخاص بتجريم الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي على جريمة الاستعمال غير المصرح به.

223 ـ أما على صعيد موقف الهيئات الدولية فيما يتعلق بتجريم الاستعمال غير المصرح به نسلط الضوء على دعوة منظمة التعاون الاقتصادي والتنمية والمجلس الأوروبي الدول الأعضاء إلى تجريم هذا السلوك.

224 ـ نشير ابتداء إلى موقف منظمة التعاون الاقتصادي والتنمية التي أوصت الدول الأعضاء بتجريم الاستعمال غير المصرح به للنظام المعلوماتي ؛ وذلك ليس فقط للإضرار التي يمكن أن تترتب على هذا الاستعمال، وإنما لقيمة الانفراد باستعمال نظم المعالجة الآلية للمعلومات بالنسبة إلى أصحابها. ولقد رأت المنظمة أن التجريم لا بد ان يقتصر على الحالات التي يعلم فيها الفاعل أنه يخترق بهذا الاستعمال الإجراءات الأمنية الموضوعة للحيلولة دون الاستعمال غير المصرح به، أما حالات الاستعمال قليلة الأهمية كاستعمال الحاسوب لإجراء بعض الحسابات الشخصية على سبيل المثال فيجب أن تخرج من دائرة التجريم. إلا إذا كان الاستعمال بغية ارتكاب جريمة معلوماتية أخرى أو إلحاق ضرر بالمجني عليه. كما أوصت اللجنة في تقريرها بضرورة تحديد كل مؤسسة عن طريق لوائحها الداخلية الحالات التي يعد فيها استعمال نظام الحاسوب غير مشروع[2].

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص229.

(2) OECD,Copmuter – Related Crime: Analysis legal Policy, Op.Cit.,P59.

مشار له عند، قورة، مرجع سابق، ص 429,428.

225 ـ أما المجلس الأوروبي فقد دعا في توصيته الدول الأعضاء إلى تجريم الاستعمال غير المصرح به للنظام المعلوماتي، وقد اقترح المجلس ثلاثة بدائل لتجريم هذا الفعل[1]:

أولاً: إذا تم استعمال النظام مع قبول الفاعل لاحتمال إلحاق خسائر كبيرة بمالك النظام أو الشخص المرخص له باستعماله، أو إلحاق ضرر بهذا النظام أو وظائفه.

ثانياً: إذا تم هذا الاستعمال بغية إلحاق خسائر بمالك النظام أو بالشخص المرخص له باستعماله أو إلحاق ضرر بهذا النظام ووظائفه.

ثالثاً: إذا ترتب على هذا الاستعمال إلحاق خسائر بمالك النظام أو بالشخص المرخص له باستعماله أو ترتب عليه ضرر أصاب هذا النظام ووظائفه

(1)The Recommendation NoR (89)q on Copmuter – Related Crime,op.cit.,pp.66 – 68.
مشار له عند، المصدر السابق، ص 430,429.

المبحث الثالث
إتلاف المعلومات

226 ـ الإتلاف هو التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له[1]. فجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من أجله.

وفعل الإتلاف في مجال المعلوماتية قد يقع على المكونات المادية للنظام المعلوماتي، وقد يقع على المكونات المعنوية لهذا النظام المتمثلة في المعلومات دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي.

227 ـ في الحالة الأولى نؤكد على أن الإتلاف الذي يقع على المكونات المادية للنظام المعلوماتي ـ كالإتلاف الذي يقع على شاشات العرض والأشرطة والاسطوانات والأقراص الممغنطة والكابلات وشبكات الربط ومعدات الإدخال والإخراج وغيرها ـ يخضع للنصوص التقليدية في قانون العقوبات الذي تناول بالتجريم فعل الإتلاف الذي يؤدي إلى إلحاق الضرر بالمال المنقول المملوك للغير وذلك في نص المادة (445) من قانون العقوبات الأردني.

228 ـ تجدر الإشارة إلى أن هناك بعض التشريعات تناولت إتلاف المكونات المادية للنظام المعلوماتي في نصوص خاصة ترتبط بالجريمة المعلوماتية، ومن هذه التشريعات على سبيل المثال قانون العقوبات الخاص بولاية كاليفورنيا الذي جرم إتلاف أنظمة المعالجة الآلية للمعلومات وتخريبها بمكوناتها المادية والمعنوية.

ويرى البعض أن هذا النمط يخرج عن إطار الجريمة المعلوماتية على اعتبار أن الأخيرة تشكل اعتداء على المعلومات ونظم معالجتها بحيث يكون ذلك عن طريق

---

(1) الصغير، مرجع سابق، ص 153. وفي نفس المعنى انظر، قشقوش، هدى، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 564.

استعمال وسائل تقنية ترتبط ببرمجة المعلومات، وانه لا حاجة بالتالي إلى إفراد نصوص خاصة بإتلاف المكونات المادية للنظام المعلوماتي حيث تكفي النصوص التقليدية في هذا المجال[1].

229 ـ ويحمد للمشرع الأردني وضع نصوص خاصة وصريحة تجرم الإتلاف المادي الذي يقع على منشآت الاتصالات التي تشمل بالضرورة شبكة الانترنت ومنشآتها المادية وذلك في قانون الاتصالات الأردني رقم (13) لسنة 1995، حيث نصت المادة (72) من هذا القانون على ما يلي:

أ- "كل من أقدم قصداً على تخريب منشآت الاتصالات أو الحق بها ضرراً عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين أو بغرامة لا تقل عن (200) دينار ولا تزيد على (5000) دينار أو بكلتا العقوبتين وتضاعف العقوبة إذا تسبب فعله بتعطيل حركة الاتصالات.

ب- كل من تسبب إهمالاً في تخريب منشآت الاتصالات أو الحق الضرر بها، يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على (100) دينار أو بكلتا العقوبتين."

230 ـ أما فيما يتعلق بالحالة الثانية وهي حالة وقوع الإتلاف على المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكات المحلية أو العالمية، فإن السؤال يثار حول الحماية التي وفرها المشرع الأردني في قانون العقوبات لهذه المعلومات من خطر الإتلاف الذي قد تتعرض له. وبناء على ما تقدم فإننا سنتناول الأساليب التقنية المستخدمة في إتلاف المعلومات في (المطلب الأول)، ثم نعرض بعد ذلك إمكانية انطباق النصوص التقليدية المتعلقة بالإتلاف في قانون العقوبات الأردني على إتلاف المعلومات في (المطلب الثاني).

---

(1) قورة، مرجع سابق، ص190.

المطلب الأول: الأساليب التقنية المستخدمة في إتلاف المعلومات

231 ـ إن القيام بإتلاف المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكات المحلية أو العالمية يؤدي إما إلى تدميرها أو محوها أو تشويهها بشكل يؤثر في قيام النظام المعلوماتي بوظائفه المعتادة.

وتتنوع أساليب إتلاف المعلومات وأنماطها ولا يمكن عملياً حصرها، حتى لو أمكن ذلك في الوقت الحاضر إلا أنه لا يمكن التنبؤ بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات.

232 ـ الاعتداءات على المعلومات بالإتلاف قد يتحقق بالإدخال غير المشروع للمعلومات أو للبرامج حيث يتم في هذه الحالة إدخال معلومات أو بيانات أو برامج لم تكن موجودة في السابق بقصد التشويش على المعلومات أو البيانات الموجودة ابتداء، الأمر الذي يؤثر على صحتها وقيمتها. ويعتبر إدخال البرامج الخبيثة إلى النظام المعلوماتي بهدف إتلاف المعلومات وتشويهها وتدميرها من أكثر الوسائل انتشاراً وخطورة على المكونات المنطقية للنظام المعلوماتي، حيث أنها تستخدم في الوقت الراهن على نطاق واسع وتسبب خسائر اقتصادية فادحة بمختلف القطاعات العامة والخاصة وذلك لسهولة انتشارها وسرعة عملها. ومن أشهر هذه البرامج الفيروسات وبرامج الدودة والقنابل المنطقية والزمنية التي سنقوم باستعراضها على التوالي.

أولاً: الفيروسات (Viruses)

233 ـ الفيروس ـ كما حدده أحد التقارير الصادرة عن المركز القومي الأمريكي للحواسيب ـ عبارة عن: (برامج مهاجمة تصيب أنظمة الحاسبات بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان)[1].

فالفيروسات: (عبارة عن برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى آخر في العالم، وهو يسمى عادة باسم أول مكان

---

(1) مشار له عند عفيفي، مرجع سابق، ص197.

اكتشف فيه، والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم حيث يصعب اكتشافها، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً يدل عليها، وعلى الرغم من تدميرها للبرامج والمعلومات إلا أنها لا تسبب عادة تدميراً لأي من المكونات المادية للنظام)[1].

234 ـ وكان أول من فكر في فيروس الحاسوب هو (جون نيومان) عام 1949 عندما طرح الفكرة الأساسية في تصميم الفيروس الالكتروني في مقال نشر له تحت عنوان "نظرية التعقيد الأوتوماتيكي" ومفاده أن جهاز الحاسوب يمكن أن يدمر نفسه، ولم يلق هذا المقال في حينه أهمية لقلة انتشار الحواسيب[2].

235 ـ تتمتع الفيروسات[3] بقدرة فائقة على مهاجمة أجهزة الحاسوب والشبكات المعلوماتية وتعطل الاتصالات وتشوه البيانات بل وتضلل المستخدم أحيانا ببيانات خاطئة، فالفيروس قد يؤدي إلى تغيير في الحقيقة أو تعديل في المعلومات.

وتشكل هذه الوسيلة التقنية المستخدمة في مجال ارتكاب الجرائم المعلوماتية رعباً وتهديداً حقيقياً لكل مستخدمي أجهزة الحاسوب وشبكة الإنترنت العالمية وذلك نظرا للتزايد الهائل في حجم الاعتماد على تقنيات نظم المعلومات لدى الأفراد والمؤسسات والشركات وكذلك الدول في تسيير الأعمال المختلفة، حيث أصبحت الحواسيب وشبكاتها اللبنة الأساسية في قيام أي دولة حديثة.

236 ـ وترتب على هذه الفيروسات باعتبارها وسيلة تقنية مستخدمة في ارتكاب جريمة تدمير نظم المعلومات وإتلافها أو تعطيلها خسائر مادية فادحة تقدر بملايين

---

(1) قورة، مرجع سابق، ص 192،191. ويعرفها د سامي الشوا على انها (عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جداً لدرجة تصيب النظام المعلوماتي بالشلل التام، او هي عبارة عن خلية كهرومغناطيسية نائمة ومبرمجة بحيث تنشط في وقت محدد لتخريب البرنامج الأصلي وتنتشر في الأجهزة الأخرى التي تضمها الشبكة بحيث تفسد ما تحويه من معلومات) الشوا. ثورة المعلومات..... مرجع سابق، ص189.

(2) منيغب، نعيم، مخاطر المعلوماتية والانترنت. (ط1). بيروت، منشورات الحلبي، 1998، ص218.

(3) تستخدم كلمة الفيروس في مجال المعلوماتية بشكل عام للدلالة على كل البرامج الخبيثة التي تسبب اتلافاً لأنظمة المعالجة الآلية للمعلومات، إلا ان الفيروس في حقيقة الأمر هو احد انواع هذه البرامج، وتتسبب هذه البرامج جميعها في إتلاف المكونات المنطقية لجهاز الحاسوب، وتستمد التفرقة بين هذه البرامج أساسها من أسلوب كل منها في أداء وظيفته.

الدولارات، فضلاً عن تعطيل الأنظمة المعلوماتية لفترة قد تطول وقد تقصر مما قد ينتج عنه خسائر ضخمة. ومن الأمثلة التي تعكس خطورة هذا النوع من الإجرام، قيام أحد المبرمجين بإطلاق فيروس من جهاز حاسوب استهدف شبكة اربانت (ARPANET) التي تربط حواسيب مؤسسات على درجة كبيرة من الأهمية مثل الجيش والجامعة وإدارة البحث العلمي في الولايات المتحدة والبريد الالكتروني وغيرها. وهذا الفيروس قام بنسخ نفسه عدة مرات في هذه الشبكة مما ألقى حملاً زائداً على ما يقدر بستة آلاف حاسوب خلال يومين مما تسبب في حدوث إقفال في الشبكة ونتجت أضرار مادية قدرها البعض بـ (96) مليون دولار أمريكي[1].

237 ـ ويستخدم الفيروس بشكل عام لتحقيق احد غرضين[2]:

1- الغرض الحمائي :

ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به، فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه ويعد ذلك بمثابة عقوبة تلحق بالناسخ.

وهناك أصابع اتهام تشير إلى أن الشركات الكبرى قد تلجأ أحيانا إلى هذه الحيلة لحماية برامجها من النقل غير المشروع الذي يهدد استثماراتها في هذا المجال، حيث يتم إطلاق هذه الفيروسات عند محاولة النقل غير المشروع[3].

2- الغرض التخريبي:

يتم إعداد هذه الفيروسات من قبل فئة مريضة من خبراء البرامج وذلك بهدف الدعاية أو الابتزاز، فيرمي صانع الفيروس إلى التخريب بحد ذاته أو إلى التخريب بهدف الحصول على منافع شخصية[4].

---

(1) انظر عفيفي، مرجع سابق، ص 199، 198.

(2) لطفي، الجرائم التي تقع على الحاسبات... مرجع سابق، ص 496.

(3) الشوا، ثورة المعلومات... مرجع سابق، ص190.

(4) من المنافع الشخصية التي قد يهدف صانع الفيروس للحصول عليها:=

238 ـ وأنواع الفيروسات تتعدد وتتنوع، ويمكن تقسيمها من حيث تكوينها وأهدافها إلى[1]:

1- فيروس عام العدوى، وهو فيروس ينتقل إلى أي برنامج أو ملف.
2- فيروس محدود العدوى، وهو يستهدف نوعاً معيناً من النظم لمهاجمته، ويتميز عن النوع السابق بأنه أبطأ في الانتشار وأصعب في الاكتشاف.
3- فيروس عام الهدف، وهو ما تندرج تحته الغالبية العظمى من الفيروسات التي تم اكتشافها حتى الآن، ويتميز بسهولة إعداده واتساع مدى تدميره.
4- فيروس محدد الهدف، وهو لا يؤدي إلى تعطيل عمل البرامج بل يؤدي إلى تغيير الهدف منها، كأن يحدث تلاعباً مالياً أو تعديلاً معيناً في تطبيق عسكري.

وفي الواقع إن المجني عليه في معظم الأحيان لا يعرف من الجاني الذي صمم الفيروس كما انه قد لا يعرف لمدة طويلة إصابة برامجه بالفيروس، كما أن المجني عليه قد لا يرغب في الإعلان عن إصابة نظامه بهذا الفيروس خصوصا إذا كانت مؤسسة مالية[2].

239 ـ ويبدو أن الفيروسات آخذة بالتزايد بشكل متسارع ويعود السبب في ذلك إلى وجود الشبكة العالمية للمعلومات (الإنترنت)، فقبل هذا الاستعمال المذهل لشبكة الانترنت كان انتشار الفيروسات في جميع أنحاء العالم يستغرق عامين إلى خمسة أعوام، أما الآن فيستغرق الأمر ساعات محدودة[3]. ومن أشهر الفيروسات الموجهة ضد الحواسيب والشبكات المعلوماتية:

1- =ابتزاز مستخدم النظام حتى يتقي خطر التدمير أو خطر التشهير بضعف نظامه الأمني، وهو ما قد يترتب عليه مثلاً عزوف عملاء البنك الذي تعرض لأحد الفيروسات عن التعامل معه.

2- التجسس على مستخدم النظام لإفشاء البيانات السرية الخاصة به. انظر، لطفي، جرائم الكمبيوتر، مرجع سابق، ص 497، 496.

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 191.

(2) عفيفي، مرجع سابق، ص 202، 201.

(3) غرير، إيرل، (1998)، أنا فيروس: فهل تسمع زئيري، مجلة بايت، العدد (3) السنة (4)، ص51.

1- فيروس الإبطاء، ويتمثل عمل هذا الفيروس في إبطاء عمل جهاز الحاسوب بصورة تدريجية تمهيداً لإيقافه عن العمل.

2- الفيروسات النائمة، وهي فيروسات خطيرة جداً وتكمن خطورتها في كونها تظل منكمشة إلى حين ثم تنطلق لتنفيذ أهدافها التخريبية.

3- الفيروسات التطورية، و هي فيروسات لها القدرة على أن تقوم بتغيير شكلها بمرور الوقت وبذلك تستطيع أن تقوم بمهمة تدمير برامج وبيانات الحاسوب دون صعوبة تذكر[1].

4- فيروس حصان طروادة، وهو عبارة عن برنامج فيروس لديه قدرة على الاختفاء في البرنامج الأصلي للمستخدم وعندما يتم تشغيل البرنامج الأصلي ينشط الفيروس المتمثل في حصان طروادة وينتشر ليبدأ نشاطه التدميري، وهذا الفيروس يؤدي إلى تعديل البرنامج وتزوير المعلومات ومحو بعضها وقد يصل إلى تدمير النظام بأكمله[2].

5- الفيروس الإسرائيلي: وهو فيروس تم اكتشافه في الجامعة العبرية في القدس، وهو يقوم بإبطاء تشغيل النظام المعلوماتي إلى نصف زمن التشغيل تقريبا بعد نصف ساعة فقط من تشغيل الجهاز[3].

240 ـ وهناك بعض الفيروسات تم تصنيعها في مناسبات معينة إما للتعبير عن الاحتفال بها أو للاحتجاج عليها، واهم هذه الفيروسات[4]:

أ- فيروس مايكل أنجلو:

أطلق هذا الفيروس يوم 6 مارس عام 1992 بمناسبة الاحتفال بذكرى ميلاد الرسام الايطالي الشهير مايكل أنجلو. وأصاب هذا الفيروس العديد من أجهزة الحاسوب الشخصية في عدد كبير من دول العالم.

---

(1) انظر حول أنواع الفيروسات، عفيفي، مرجع سابق، ص 202،203. وكذلك، رضوان، رضا عبد الحكيم، (1999). التقنيات العلمية في مكافحة فيروسات الكمبيوتر. مجلة الأمن والحياة. العدد (204). ص58 ـ 60

(2) قشقوش، جرائم الحاسب الالكتروني... مرجع سابق، ص 120،121.

(3) الشوا، ثورة المعلومات... مرجع سابق، ص193. وكذلك، عبابنة، محمود، الحماية الجنائية لمعلومات وبرامج الحاسوب، بحث مقدم لمؤتمر القانون والحاسوب، جامعة اليرموك، اربد، الفترة من 12 ـ 14 تموز (2004)، ص13.

(4) انظر، الشوا، ثورة المعلومات... مرجع سابق، ص 193،192. وكذلك، عفيفي، مرجع سابق، ص 204.

ب- فيروس ناسا:

وهو فيروس أطلق احتجاجا على إنتاج الأسلحة النووية. فهو عبارة عن برنامج يحمل رسالة مناهضة للأسلحة النووية وتظل هذه الرسالة تكرر نفسها وتتكاثر بشكل مدمر للبرامج الأخرى.

241 ـ ويوجد هناك مصادر متعددة أو محتملة للفيروسات على اختلاف أنواعها، فقد يكون مصدر هذه الفيروسات[1]:

- الموظفون القائمون على تصميم البرامج أو تشغيلها، حيث يقوم هؤلاء الموظفون بصنع فيروسات بهدف الانتقام من المؤسسة التي يعملون بها أو لمجرد إثبات المهارة والكفاءة.
- الجاسوسية العسكرية والصناعية، فقد تقوم أجهزة المخابرات في بعض الدول أو الشركات الصناعية بإدخال فيروس إلى البرنامج المراد التجسس عليه وذلك للحصول على معلومات صناعية أو عسكرية.
- الإرهاب، فقد تقوم الجماعات الإرهابية المنظمة باستخدام نظم الاتصالات الحديثة في تنفيذ مخططاتها الإرهابية عن بعد، فتقوم بصنع فيروسات بهدف تخريب وإتلاف الأهداف التي تعتقد أنها تقف ضد مبادئها ومعتقداتها.
- كذلك فإن قراصنة الحاسوب قد يكون لهم دور في انتشار هذه الفيروسات وكذلك المتنافسين في مجال صناعة الحواسيب وغير هؤلاء ممن لهم مصلحة في انتشار هذه الفيروسات وتدميرها لنظم المعلومات المختلفة.

ثانياً: برامج الدودة (Worm Software)

242 ـ وهذه البرامج تكون مصممة للانتقال عبر شبكات الاتصال من جهاز إلى آخر وهو ما يؤدي إلى عجز النظام المعلوماتي عن أداء عمله عن طريق محو عدة أجزاء من المعلومات.

---

(1) انظر، عفيفي، مرجع سابق، ص 200،201. وكذلك، الرومي، مرجع سابق، ص 60،61.

فهذه الوسيلة التقنية تؤدي إلى تعطيل وإيقاف النظام المعلوماتي بصورة كاملة فهذا الفيروس ينسخ نفسه عدة مرات.

والدودة المعلوماتية تنتشر أساساً عبر خطوط التوصيلة الالكترونية وتصدر معلومات غير صحيحة وتؤدي في النهاية إلى إغلاق النظام[1].

243 ـ وفيروس الدودة يصيب جزءاً محدداً من نظام المعالجة الآلية للبيانات وهو الجزء الخاص بنظام التشغيل (Operating System) والذي يقصد به مجموعة البرامج التي تتحكم في إمكانيات الحاسوب وفي العمليات التي تستخدمها هذه الإمكانيات[2].

244 ـ تهدف برامج الدودة إلى شغل أكبر حيز ممكن من سعة الشبكة ومن ثم العمل على تقليل أو خفض كفاءتها، وأحيانا تتعدى هذا الهدف لتبدأ بعدها بالتكاثر والانتشار في التخريب الفعلي للملفات والبرامج ولنظم التشغيل[3].

245 ـ وفي الواقع العملي يمكن أن نشير إلى بعض الأمثلة لاستخدام برامج الدودة في إتلاف المعلومات وتدميرها منها:

- قيام طالب جامعي ألماني في ديسمبر 1987 بإرسال بطاقة تهنئة من خلال إحدى الحاسبات وقد صمم لهذا الغرض برنامج دودة قادر على قراءة العناوين الموجودة بذاكرة الحاسوب، وقام بنسخ بطاقة التهنئة إلى نسخ كثيرة حيث أرسلها إلى كل العناوين التي قرأها البرنامج الأمر الذي أدى بعد اختراقه لشبكة (Vnet) ـ التي تربط حاسبات 45 دولة ـ إلى تغطية نصف مليون حاسوب خلال ساعتين فقط مما أدى إلى تعطيلها لمدة 48 ساعة تقريبا[4].

---

(1) قشقوش، جرائم الحاسب الالكتروني... مرجع سابق، ص 122.

(2) المصدر السابق، ص 123.

(3) الشوا، ثورة المعلومات... مرجع سابق، ص 193.

(4) انظر، عفيفي، مرجع سابق، ص 206، 205.

- قيام طالب دراسات عليا أمريكي يدعى (روبرت مورس) بإعداد برنامج عرف باسم (Internet Warm) تمكن من خلاله من تدمير وإلحاق أضرار بـ (16) ألف شبكة حاسبات واسعة الانتشار في الولايات المتحدة الأمريكية، الأمر الذي أسفر عن خسائر مالية قدرت بعدة ملايين من الدولارات[1].
- قيام بعض الأشخاص بصنع برامج دودة سميت " بالبرامج الدودية ضد القتلة مستخدمي الذرة " وذلك احتجاجاً منهم على قيام الولايات المتحدة الأمريكية بإطلاق مكوك فضائي يحمل مجساً فضائياً مغطى ببودرة نووية، حيث استهدفت هذه البرامج شبكة حاسوب علوم الأرض والفضاء في الولايات المتحدة الأمريكية[2].

ثالثاً: البرامج (القنابل) المنطقية والزمنية

246 ـ أو ما يسمى بالقنبلة المعلوماتية، وهو اصطلاح يطلق على أنواع من البرامج المعلوماتية التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف. وتنقسم القنبلة المعلوماتية إلى قسمين:

1- القنابل المنطقية:

247 ـ وهي برامج تظل خاملة إلى أن تتحقق لها بعض الشروط فتتفجر وتدمر الملفات الموجودة داخل جهاز الحاسوب.

ويمكن القول أنها: (عبارة عن برنامج أو جزء من برنامج، ينفذ في لحظة محددة أو في كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع)[3].

---

(1) انظر الشوا، ثورة المعلومات... مرجع سابق، ص 194، وكذلك عفيفي، مرجع سابق، ص 206.

(2) راجع الشوا، ثورة المعلومات... مرجع سابق، ص 194.

(3) الشوا، ثورة المعلومات...... مرجع سابق، ص 194.

248 ـ والقنابل المنطقية تظل في حالة سكون ولا يتم اكتشافها مدة من الزمن قد تطول أو تقصر وهذه المدة يحددها المؤشر الموجود داخل برنامج القنبلة.

وهذا المؤشر لا يقتصر على المدة الزمنية، وإنما قد يمتد إلى ما يعرف بتوافر شروط منطقية معينة داخل برنامج أو ملف معين وذلك حسب الرمز الذي يحدده البرنامج القنبلة فإذا حل الميعاد أو توافرت هذه الشروط بدأ البرنامج في القيام بمهامه التخريبية[1].

249 ـ ومن الأمثلة الواقعية على وضع قنابل منطقية في النظام المعلوماتي من أجل تدمير المعلومات وإتلافها:

- قيام أحد المبرمجين في ولاية تكساس الأمريكية سنة 1985 بوضع قنبلة منطقية في حاسوب الشركة التي كان يعمل بها بعد فصله منها مستغلاً عدم تغيير الشركة كلمة السر التي كان يعرفها، مما أدى إلى تدمير سجلات عمولة المبيعات مرة كل شهر[2].
- تمكن خبير في نظم المعلومات في الدنمارك من وضع قنبلة منطقية في نظام أحد الحواسيب أدت إلى محو أكثر من مائة برنامج، وقد تم أيضاً محو النسخ الاحتياطية عند تشغيلها نظراً لانتقال أثر القنبلة إليها. وقد تم ضبط المجرم وحكم عليه القضاء الدنماركي بالسجن لمدة سبعة أشهر.

2- القنبلة الزمنية أو الموقوتة:

250 ـ وهي عبارة عن برامج يتم إدخالها بطرق مشروعة متخفية مع برامج أخرى، وتهدف إلى تدمير برامج ومعلومات النظام وتغييرها وتعمل على مبدأ التوقيت حيث تنفجر في وقت معين[3].

251 ـ استخدام القنابل الزمنية (الموقوتة) يحقق أهدافاً متعددة لمعديها منها:

---

(1) عفيفي، مرجع سابق، ص 207.

(2) راجع، عفيفي، مرجع سابق، ص 208.

(3) اكرم عيسى، انواع جرائم الحاسوب، جريدة الدستور، عمان، عدد 11091، (20 ـ 1 ـ 2001)، ص 28. وانظر في نفس المعنى، المناعسة وآخرون، مرجع سابق، ص 157.

- يمكن من خلال هذه القنابل توقيت القيام بعملية التخريب في وقت معين يلحق اكبر ضرر ممكن بنظام الحاسوب.
- من شأن تأجيل التفجير أن يجعل التوصل إلى معدي هذه البرامج متعذراً إن لم يكن في بعض الأحيان مستحيلاً.
- التأجيل يتيح انتقال القنبلة للنسخ الاحتياطية للبرامج التي تقوم الجهة المستهدفة بإعادة إنتاجها.

252 ـ من الأمثلة على استخدام القنبلة الزمنية في الواقع العملي من أجل تدمير المعلومات وإتلافها:

قيام أحد المبرمجين الفرنسيين بوضع قنبلة موقوتة في شبكة المعلومات في الجهة التي كان يعمل بها أثر فصله من العمل. وهذه القنبلة كانت تتضمن أمراً بتفجيرها بعد ستة أشهر من تاريخ فصله، الأمر الذي نتج عنه تدمير كلّ بيانات هذه الجهة[1].

المطلب الثاني: الحماية الجنائية للمعلومات من الإتلاف في قانون العقوبات الأردني

253 ـ عالج المشرع الأردني في قانون العقوبات جريمة الإتلاف والتخريب في الفصل السادس من الباب الحادي عشر تحت عنوان الأضرار التي تلحق بأملاك الدولة والأفراد. وقد أوضحت المواد التي عالجت هذه الجريمة أن الإتلاف والتخريب لا يقع إلا على العقارات والأموال المنقولة.

254 ـ ويشير نص المادة (445) من قانون العقوبات إلى أن: (كل من الحق باختياره ضرراً بمال غيره المنقول، يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين)[2].

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص196.

(2) يقابله نص المادة (361) من قانون العقوبات المصري والذي جاء فيه: (كل من خرب او اتلف عمداً اموالاً ثابتة او منقولة لا يمتلكها او جعلها غير صالحة للاستعمال او عطلها باية طريقة يعاقب بالحبس مدة لا تزيد على ستة اشهر وبغرامة لا تتجاوز ثلاثمائة جنيه او باحدى هاتين العقوبتين)، ويقابله كذلك نص المادة (733) من قانون العقوبات=

ويتضح من نص المادة السابقة أن أركان جريمة الإتلاف تتمثل في الركن المادي ومحل الجريمة والركن المعنوي.

255 ـ فيما يتعلق بالركن المعنوي فهو لا يثير أي صعوبة من الناحية القانونية، فجريمة الإتلاف جريمة عمدية تقوم على توافر القصد الجنائي العام المتمثل بعلم الجاني بعناصر الجريمة وأركانها وأنه يقوم بإتلاف مال الغير واتجاه إرادته كذلك للقيام بهذا الفعل.

256 ـ أما فيما يتعلق بالركن المادي لجريمة الإتلاف، فانه يتمثل بالنشاط الإجرامي الذي يقوم به الجاني ويكون من شأنه إلحاق ضرر بمال الغير المنقول. وهذا النشاط الإجرامي قد يكون في جعل المال غير قابل للإصلاح أو للاستعمال أو قد يكون بالتأثير في مادة الشيء على نحو يقلل من قيمته الاقتصادية أو قد يكون بتعطيل الشيء أي إعاقته عن العمل كلياً أو جزئياً.

257 ـ أما محل الجريمة فهو المال المنقول المملوك للغير. وفي الواقع فان العقبة التي تحول دون تطبيق نص المادة (445) على جريمة إتلاف المعلومات هي طبيعة المحل في هذه الجريمة، فإذا كنا قد توصلنا سابقاً إلى أنه لا يوجد ما يمنع من انطباق وصف المال على المعلومات، فإن المشكلة تكمن هنا في وصف المال بأنه منقول، فهل يقتصر نص المادة (445) على المنقولات المادية دون المعنوية؟

258 ـ لم يتطرق قانون العقوبات الأردني إلى تعريف المنقول أو العقار وبالتالي كان لا بد من الرجوع إلى القانون المدني الأردني، الذي حدد مدلول العقار في المادة (58) التي أشارت إلى أن: (كل شيء مستقر بحيزه ثابت فيه لا يمكن نقله منه دون تلف أو تغيير هيئته فهو عقار، وكل ما عدا ذلك من شيء فهو منقول).

=اللبناني، والتي جاء فيها: (كل من هدم أو خرب قصداً شيئاً يخص غيره مما لم يعين في هذا الباب يعاقب بغرامة لا تجاوز قيمة الضرر على أن لا تنقص عن عشر ليرات، وإذا كانت قيمة الشيء المتلف أو الضرر الناجم يجاوز المائة ليرة فيمكن علاوة على الغرامة أن يحبس الفاعل مدة لا تفوق الستة أشهر).

أي أن المنقول هو: (كل شيء ليس له مستقر ثابت ويمكن نقله وتحويله من مكانه دون تلف فيه أو تغيير في هيئته)[1]. والمنقول قد يكون مادياً وقد يكون معنوياً، باعتبار أن المنقول بحسب الأصل مال، والمال قد يكون مادياً أو قد يكون معنوياً[2].

259 ـ ويلاحظ أن القانون الجنائي قد توسع في معنى المال المنقول الخاضع للحماية الجزائية، فقد صنف فقهاء القانون الجزائي المال المنقول إلى ثلاثة أنواع رئيسية هي[3]:

1- المنقولات المادية وهي الأشياء التي تكون مستقلة في وجودها كالسيارات وغيرها.
2- العقارات بالاتصال وهي عبارة عن منقولات مادية اكتسبت صفة العقار نتيجة اتصالها بعقار، حيث إذا فصلت هذه الأموال عن العقار الذي اتصلت به عادت إلى صفتها الأصلية وهي المنقول.
3- العقار بالتخصيص وهو عبارة عن منقولات بطبيعتها خصصها حائزها القانوني لخدمة عقار محدد ونتيجة هذا التخصيص اكتسبت صفة العقار.

260 ـ يرى البعض:[4] إن المعلومات والبرامج يمكن أن تكون محلاً لجريمة الإتلاف ذلك أن المشرع قد نص على أن محل الجريمة هي الأموال المنقولة، وهي لا تقتصر على الأموال المادية. مما يعني أنها تنطبق على الأموال المنقولة المادية والمعنوية، فالنص جاء بعبارات عامة بصدد المنقول.

---

(1) الداودي، غالب علي، المدخل إلى علم القانون، ط6، دار وائل للطباعة والنشر، عمان، 1999، ص 274.

(2) عفيفي، مرجع سابق، ص 110.

(3) نجم وصالح، مرجع سابق، ص 324.

(4) انظر في ذلك:

- المناعسة وآخرون، مرجع سابق، ص 156.
- عفيفي، مرجع سابق، ص 188.

كذلك يرى أنصار هذا الاتجاه أن القول بغير ذلك يترتب عليه أن تكون المعلومات مجردة من أي حماية جنائية الأمر الذي يفتح المجال على مصراعيه للاعتداء عليها.

261 ـ ويذهب آخرون[1] إلى أن المعلومات بذاتها لا يمكن أن تكون محلاً لجريمة الإتلاف؛ ذلك أن المعلومات المبرمجة آليا بمثابة نبضات كهربائية تفتقر إلى الطبيعة المادية.

فالمشرع بتجريمه فعل الإتلاف يحمي حق الملكية، العقارية أو المنقولة، وهو يحميه عن طريق حماية موضوعه من الأفعال التي تفني مادته أو قيمته في صورة كلية أو جزئية، فتقضي أو تنقص تبعاً لذلك من منفعة الشيء لمالكه، ويتعين أن يكون لذلك الشيء طبيعة مادية. وعلى الرغم من أن الشارع لم يصرح بهذا الشرط فهو مستخلص من وقوع هذه الجريمة على حق الملكية وهذا الحق كسائر الحقوق العينية لا ينصب إلا على أشياء ذات كيان مادي[2]. ويستخلص من ذلك أن الأموال المعنوية غير المتجسدة في كيان مادي ملموس ومحسوس لا تصلح محلاً لجريمة الإتلاف.

كذلك فان الحجة القوية التي تساند هذا الرأي هي التي تقوم على ضرورة تجنب التفسير الواسع للنصوص الجنائية أو الاجتهاد أو القياس عليها بشكل يخرج بها عن قاعدة الشرعية، إذ ليس هناك مبرر للانكفاء على نص ما بغية تحميله مالا يحتمل

---

(1) من انصار هذا الاتجاه:

- كامل السعيد. جرائم الكمبيوتر... مرجع سابق، ص 244،245.
- جميل الصغير. مرجع سابق، ص 156وما بعدها.
- نائلة قورةمرجع سابق، ص 194.
- يونس عرب. دليل امن.... مرجع سابق، ص453 وما بعدها.
- عمر الحسيني. مرجع سابق، ص77.
- غالي، عبدالكريم، (2001). الحماية الجنائية للمعلوميات على ضوء القانون المغربي. بحث مقدم لمؤتمر الوقاية من الجريمة في عصر العولمة، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، ص15.

(2) حسني. مرجع سابق، ص 488، 487.

فالنص الجنائي يجب أن ينطبق على الواقع بسلاسة وسهولة وليس بشد طرف من هنا وجذب طرف آخر من هناك[1].

262 ـ ونحن من جانبنا نؤيد ما ذهب إليه أصحاب الاتجاه الثاني، فبالرغم من أهمية حماية المعلومات من أفعال الإتلاف والتخريب إلا أن الحل لا يكون في التوسع في تفسير النصوص التقليدية، بل يستلزم الأمر توفير حماية للمعلوماتية عن طريق نصوص تشريعية خاصة تراعي خصوصية المعلومات والتي تختلف عن الأموال المادية الملموسة التي وضعت نصوص قانون العقوبات ابتداء لحمايتها.

263 ـ تجدر الإشارة إلى أن المشرع الأردني في قانون الاتصالات رقم (13) لسنة 1995 كفل نوعاً من الحماية للمعلومات والبيانات المتبادلة عبر شبكات الاتصال من خطر الإتلاف حيث نصت المادة (76) من القانون المذكور على ما يلي:

(كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر، أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين).

كما نصت المادة (77) أن: (كل من أقدم على كتم رسالة عليه نقلها بواسطة شبكات الاتصال إلى شخص أو رفض نقل رسائل طلب منه نقلها من قبل المرخص له أو الهيئة أو نسخ أو أفشى أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة و الرسائل المرسلة أو المستقبلة، يعاقب بالحبس لمدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على ألف دينار أو كلتا العقوبتين).

264 ـ ونلاحظ أن الدول الأخرى ـ وخاصة المتقدمة منها في مجال التعامل مع المعلوماتية ـ قد وضعت نصوصاً صريحة تجرم الأفعال التي تستهدف إتلاف المعلومات ومن هذه الدول فرنسا والولايات المتحدة الأمريكية وكندا[2].

---

(1) الحسيني، مرجع سابق، ص 75.

(2) حيث نصت المادة (3/323) من قانون العقوبات الفرنسي على أنه (يعاقب بالحبس مدة تتراوح بين ثلاثة أشهر وثلاث سنوات وبغرامة مقدارها (30.000) فرنك أو بإحدى هاتين العقوبتين كل من ادخل عمداً إلى نظام المعالجة الآلية للمعلومات بطريق مباشر أو غير مباشر دون مراعاة حقوق الغير، بيانات أو محى أو عدل في البيانات التي يحويها النظام أو في طرق معالجتها أو نقلها) مشار لهذا النص عند، قورة، مرجع سابق، ص 209.

265 ـ وأهم ما يميز النصوص الفرنسية والأمريكية التي جرمت إتلاف المعلومات أنها تخلت عن اشتراط صفة المنقول أو العقار في المال الواقع عليه فعل الإتلاف، واكتفت بتوافر الصفة المالية للشيء الواقع عليه فعل الإتلاف[1].

(1) الحسيني، مرجع سابق، ص 75.

المبحث الرابع
تــزويــر المـعــلومـــات

266 ـ حـرص المـشرع الجزائـي في دول العـالم المختلفـة علـى تجـريم التزويـر في المحررات إيمانا منه بأن التزوير في المحررات يهدد الثقة العامة للأفراد بها وبالتالي يخل باليقين والاستقرار في المعاملات وسائر نواحي الحياة القانونية في المجتمع.

267 ـ وعلة ذلك أن المحرر المكتوب يعتبر وسيلة أساسية من وسائل الإثبات المدنية والتجارية في كل الأمور التي تتطلب إثباتاً بالكتابة، فالأشخاص يعتمدون على الأدوات المكتوبة لإثبات علاقاتهم، و المحررات هي الوسيلة كذلك لحسم المنازعات واثبات الحقوق ولا يتاح للكتابة هذا الدور المهم الذي تقوم به إلا إذا منحها الناس ثقتهم[1].

268 ـ وفي نطاق مجتمع المعلوماتية الحديث أصبح الحاسوب ونظامه المعلوماتي جزءاً لا يتجزأ من حياة الأفراد اليومية، بل أنه أصبح يحل محل الأوراق في العديد من مجالات الحياة مثل عمليات الدفع وطلبيات البضائع وتحويل الأموال من مصرف إلى آخر[2]، كما أن معظم الهيئات الحكومية وهيئات القطاع الخاص تعتمد على الحاسوب في تسيير أعمالها، فالحواسيب تستخدم لحفظ المستندات ومعالجتها آليا.

وفي ظل هذا الانتشار المتزايد لتقنية المعلومات أصبح هناك قلق متزايد من ارتكاب جرائم تزوير البيانات والمعلومات المخزنة أو المنقولة عبر شبكة الإنترنت، أو أن يتم تزوير مستخرجات النظام المعلوماتي من مستندات أو شرائط ممغنطة أو دعامات مسجل عليها المعلومات.

---

(1) تمام، احمد حسام، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، 2000، ص387.

(2) الصغير، مرجع سابق، ص 162.

269 ـ إن ارتكاب جريمة التزوير المعلوماتي سيكون لها ـ ودون أدنى شك ـ انعكاس سلبي على الثقة التي يوليها الأفراد للنظام المعلوماتي وما يحتويه من معلومات وما يتم استخراجه منه.

والمسألة التي تثار في هذا الصدد هي حول الحماية التي يوفرها القانون الجنائي من خلال قانون العقوبات الأردني لهذه البيانات والمعلومات من أخطار التزوير المعلوماتي، وهل بالإمكان أن تشمل النصوص التقليدية لجريمة التزوير في قانون العقوبات التزوير المعلوماتي؟

للإجابة عن هذا التساؤل سنتناول ابتداء الأركان العامة لجريمة التزوير في قانون العقوبات الأردني في (المطلب الأول) وفي (المطلب الثاني) نتناول مدى إمكانية انطباق هذه النصوص على التزوير المعلوماتي.

المطلب الأول: الأركان العامة لجريمة التزوير التقليدية في قانون العقوبات الأردني

270 ـ عالج المشرع الجزائي الأردني جريمة التزوير في قانون العقوبات في الفصل الثاني من الباب الخامس تحت عنوان (في الجرائم المخلة بالثقة العامة)، حيث عرفت المادة (260) التزوير أنه: (تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي).

وذلك بخلاف بعض التشريعات الأخرى التي لم تعرف التزوير إنما اكتفت ببيان الطرق التي يقع بها، كما هو الحال في القانون الفرنسي والمصري.

271 ـ وفي الفقه تم تعريف التزوير أنه: (تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يرتب ضرراً للغير، بنية استعمال هذا المحرر فيما أعد له) [1].

---

(1) حجازي، الدليل الجنائي والتزوير... مرجع سابق، ص 135.

272 ـ استناداً إلى نص المادة (260) من قانون العقوبات الأردني يتبين لنا أن الأركان التي تقوم عليها جريمة التزوير هي:

1- الركن المادي، ويقوم على وجود تحريف مفتعل للحقيقة يتم بإحدى الطرق الحصرية المنصوص عليها في القانون، وأن يقع هذا التحريف في وقائع أو بيانات يراد إثباتها ضمن صك أو مخطوط.
2- ركن الضرر المادي أو المعنوي أو الاجتماعي.
3- القصد الجرمي.

وسوف نقوم بتناول هذه الأركان الثلاثة بشيء من التفصيل:

أولاً: الركن المادي

273 ـ حتى يقوم الركن المادي في جريمة التزوير لا بد من تحريف مفتعل للحقيقة وهو اللفظ الذي استخدمه المشرع الجزائي الأردني، بينما استخدمت التشريعات الأخرى لفظ تغيير الحقيقة.

ويذهب الدكتور كامل السعيد إلى أن (التشريعات الجزائية الأخرى قد استعملت التعبير الاصوب؛ لأن لفظة التحريف تنصرف في الأغلب إلى التزوير المادي أو إحدى صوره. فالتحريف يعني لغوياً: افتراض شيء موجود على صورة معينة تم تحريفه ليصبح على صورة معينة أخرى، في حين أن التزوير في المحررات أهم وأشمل من ذلك فقد يتم التحريف في شيء موجود وقد يصطنع شيئاً غير موجود، لكن هذا لا يعني أن المشرع الأردني لا يعتبر الاصطناع تزويراً، فالاصطناع مجرم صراحة بمقتضى المادة (1/262) من قانون العقوبات ولكننا نشير إلى أن المشرع لا بد أن يتوخى الدقة)[1].

274 ـ تحريف الحقيقة أو تغيير الحقيقة هو الأساس الذي تقوم عليه جريمة التزوير، وهو يعني استبدال الحقيقة بما يخالفها وإذا انتفى ذلك العنصر فلا تقوم جريمة التزوير، كأن يقوم احدهم بإثبات بيانات مطابقة للحقيقة فلا تقوم جريمة

(1) السعيد، كامل، شرح قانون العقوبات الأردني (الجرائم المضرة بالمصلحة العامة)، بدون ناشر، 1997، ص18.

التزوير حتى لو كان ذلك الشخص يعتقد بعدم صحة هذه البيانات حتى لو ترتب على صحة فعله ضرر في حق الغير[1].

وينبني على أن التزوير يقوم على استبدال الحقيقة بغيرها إن التغيير لا يعتبر تزويراً إذا كان من شأنه أن يعدم ذاتية المحرر وقيمته، مثل محو كل الكتابة التي في المحرر أو شطبها كلها بحيث تصبح غير مقروءة أو غير صالحة للاحتجاج بها أو للانتفاع بها وإنما يعتبر الفعل في هذه الحالة إتلافاً لسند[2].

275 ـ ليس المقصود بتغيير الحقيقة تغيير الحقيقة المطلقة إنما يكفي تغيير الحقيقة القانونية النسبية، بمعنى أن جريمة التزوير تقع إذا اثبت في المحرر ما يخالف إرادة صاحب الشأن الذي يعبر المحرر عن إرادته[3].

276 ـ تغيير الحقيقة الذي تتطلبه جريمة التزوير لا بد أن يكون فيه مساس بحقوق الغير وبمراكزهم القانونية الثابتة في تلك المحررات. والتغيير قد يكون كلياً أو جزئياً، فلا يشترط أن تكون كل بيانات المحرر مخالفة للحقيقة فيكفي أن يكون بعضها غير صحيح.

277 ـ تغيير الحقيقة الذي يعتد به في جريمة التزوير لا بد أن يكون في الوقائع و البيانات التي يتضمنها الصك أو المخطوط أو المستند.

وكل محرر مخطوط باليد يطلق عليه مصطلح مخطوط، أما المستند فيقصد به كل محرر يمكن أن يستند إليه في توثيق حق أو دعمه حالة قانونية. أما الصك فالمقصود به كل محرر يتضمن الإقرار بالمال أو غير ذلك[4].

---

(1) حجازي، الدليل الجنائي والتزوير... مرجع سابق، ص 137.

(2) الصغير، مرجع سابق، ص 163.

(3) وبناء على ذلك تقع جريمة التزوير ممن يقدم شكوى في حق آخر إلى جهة مختصة، إذا وضع عليها توقيع شخص آخر ولو كان ما دون بالشكوى صحيحا ؛ لان التوقيع على الورقة للإيهام بأن ما دون فيها صادر عن صاحب التوقيع هو بذاته مغاير للحقيقة، فالجاني بهذه الحالة يكون قد نسب إلى صاحب التوقيع أمراً لم تتجه إليه إرادته. انظر، المصدر السابق. ص 164، 163 وكذلك، العقاد، محمد، جريمة التزوير في المحررات للحاسب الآلي، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 391.

(4) السعيد، شرح قانون العقوبات... مرجع سابق، ص 77، 76.

278 ـ وعليه فان تغيير الحقيقة لا بد أن يكون في محرر، والمقصود بالمحرر هو كل مستور يتضمن علامات ينتقل بها الفكر لدى النظر إليها من شخص إلى آخر[1].

ويعرف المحرر كذلك بأنه كل مكتوب يفصح عن شخص من صدر عنه ويتضمن ذكراً لواقعة أو تعبيراً عن إرادة، ويكون من شأنه إنشاء مركز قانوني معين أو تعديله أو إنهاؤه أو إثباته[2].

279 ـ والمحرر محل جريمة التزوير يتسم بثلاث سمات:

1- المحرر محل جريمة التزوير يتخذ شكلاً كتابياً، ولا يشترط أن تكون الكتابة بلغة معينة، فقد تكون لغة وطنية أو أجنبية، فلا تقوم جريمة التزوير إذا تم تغيير الحقيقة عن طريق القول أو الإشارة أو الفعل.

ولا عبرة بالمادة التي دون عليها المحرر فقد تكون من الورق أو من الجلد أو القماش أو الخشب. وحيث أن دور المحرر في التعامل يقتضي أن يتمتع بقدر من الثبات حتى يتم الرجوع إليه كلما اقتضى الأمر ذلك فلا بد أن تكون الأداة التي يدون عليها المحرر صالحة لتحقيق هذا الثبات، وبالتالي تنتفي فكرة المحرر عن الكتابة التي تدون على الجليد أو الرمال[3].

والكتابة في المحرر لا بد أن تكون واضحة بشكل يمكن معه إدراك مضمونها، فإذا استحالت قراءة المحرر بشكل كلي فلا يصلح وسيلة للإثبات وبالتالي لا يصلح محلاً لجريمة التزوير[4].

2- يجب أن تكون الكتابة في المحرر منسوبة إلى شخص معين أو جهة معينة بحيث يمكن إسناد الأفكار أو المعاني التي يشملها المحرر إلى هذا الشخص أو تلك الجهة. وبالتالي لا بد أن يكون صاحب المحرر معروفاً أو يمكن

---

(1) الصغير، مرجع سابق، ص 164.

(2) حجازي، الدليل الجنائي... مرجع سابق، ص 165.

(3) الصغير، مرجع سابق، ص 166، 167. وكذلك، السعيد، شرح قانون العقوبات... مرجع سابق، ص 78.

(4) الشوا، ثورة المعلومات... مرجع سابق، ص 156.

تمييزه، وكل شك يدور حول معرفته يسلب المحرر مظهره القانوني ووظيفته في الإثبات[1].

3- أن يحدث المحرر أثراً قانونياً، فيجب أن يتضمن المحرر محل جريمة التزوير تعبيراً عن الإرادة وإثباتاً للحقيقة، فإذا لم تكن الكتابة صالحة لإحداث أثر قانوني فاستبدالها بغيرها أو تحريفها أو اصطناعها لا يعد تزويراً، فالحماية القانونية تنصب على المراكز القانونية المرتبطة بالمحرر[2].

280 ـ والتزوير لا بد أن يقع بالطرق التي حددها قانون العقوبات على سبيل الحصر، والتزوير يكون على نوعين:

1- التزوير المادي:

وهو تغيير الحقيقة بطريقة مادية تترك أثراً يدركه البصر[3]. وتجدر الإشارة إلى أن المشرع الأردني وفي المادة (262) من قانون العقوبات الأردني حدد طرق التزوير المادي وهي[4]:

1- إساءة استعمال إمضاء أو ختم أو بصمة إصبع.
2- صنع صك أو مخطوط.
3- تغيير في مضمون الصك أو المخطوط عن طريق الحذف أو الإضافة.

2- التزوير المعنوي:

وهو تغيير الحقيقة في معنى المحرر أو مضمونه أو محتواه دون أن يمس ذلك شكله أو مادته.

والتزوير المعنوي غالباً ما يقع عند إنشاء المحرر، وهناك صعوبة في إثباته على عكس التزوير المادي الذي يثبت من فحص المحرر نفسه. أما التزوير المعنوي فهو يثبت من أمور أخرى تتيسر أحياناً وتتعذر في أحيان أخرى[5].

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 156.
(2) عفيفي، مرجع سابق، ص 225. و في نفس المعنى أنظر، الشوا، ثورة المعلومات... مرجع سابق، ص 157، 156.
(3) عفيفي، مرجع سابق، ص 232.
(4) لمزيد من التفاصيل راجع، السعيد، شرح قانون العقوبات... مرجع سابق، ص 39 ـ 63.
(5) حجازي، الدليل الجنائي.... مرجع سابق، ص 203.

حدد المشرع الأردني طرق التزوير المعنوي في المادة (263) من قانون العقوبات الأردني وهي[1]:

1- إساءة استعمال إمضاء على بياض اؤتمن عليه المزور.
2- تدوين المزور عقوداً أو أقوالاً غير التي صدرت عن المتعاقدين أو التي أملوها.
3- إثبات وقائع كاذبة على أنها صحيحة أو وقائع غير معترف بها على أنها معترف بها.
4- تحريف أية واقعة أو إغفاله أمراً أو إيراده على وجه غير صحيح.

ثانياً: ركن الضرر

281 ـ سندا للمادة (260) من قانون العقوبات الأردني فإن تغيير الحقيقة لا يعد تزويراً إلا إذا توافر ركن الضرر، ولم يشترط القانون الأردني وقوع الضرر بالفعل بل اكتفى باحتمال وقوعه.

282 ـ والضرر هو إخلال بحق أو مصلحة يحميها القانون، وقد يكون الضرر ضرراً مادياً أو معنوياً أو ضرراً فردياً أو اجتماعياً وقد يكون كذلك ضرراً محتملاً أو محققاً.

283 ـ والضرر المعنوي أو الأدبي هو الضرر الذي يصيب الإنسان في شرفه وعرضه وكرامته. أما الضرر المادي، فهو الضرر الذي يصيب الإنسان في ذمته المالية الأمر الذي يترتب عليه الإنقاص من عناصرها الايجابية أو الزيادة في عناصرها السلبية[2].

284 ـ ويعرف الضرر الفردي أو الخاص أنه: "الضرر الذي يصيب شخصاً أو جهة معينة بالذات أو هيئة خاصة". أما الضرر الاجتماعي أو العام فهو: "الضرر الذي يصيب المجتمع أو المصلحة العامة".

---

(1) لمزيد من التفاصيل راجع، السعيد، شرح قانون العقوبات... مرجع سابق، ص 63 ـ 76.

(2) السعيد، شرح قانون العقوبات... مرجع سابق، ص 89.

285 ـ والمقصود بالضرر المحتمل، هو الضرر الذي لم يتحقق بعد ولكن احتمال تحققه قائم وفقاً للمجرى العادي للأمور[1]، ففي جريمة التزوير يكفي الشروع في استعمال السند المزور[2]. أما الضرر المحقق، فهو الضرر الذي يتحقق باستعمال السند المزور فعلاً.

والقول بمدى توافر ركن الضرر أمر يعود تقديره لقاضي الموضوع حسب ظروف كل دعوى.

ثالثاً: الركن المعنوي (القصد الجنائي)

286 ـ التزوير من الجرائم العمدية التي يتخذ ركنها المعنوي صورة القصد الجنائي، الذي يقوم على توافر القصد الجنائي العام والقصد الجنائي الخاص.

1- القصد الجنائي العام الذي يقوم على ضرورة توافر عنصري العلم والإرادة، فلا بد أن يدرك الجاني أنه يقوم بتحريف مفتعل للحقيقة في صك أو مخطوط أو مستند، وإجمالاً بمحرر وذلك بإحدى الطرق المادية أو المعنوية التي نص عليها قانون العقوبات الأردني على سبيل الحصر، ولا بد أن يكون الجاني مدركاً أن هذا التزوير سيترتب عليه ضرر محقق أو احتمالي. أي لا بد من أن يكون الفاعل على علم بجميع عناصر جريمة التزوير.

   وعلم الجاني وحده لا يكفي لقيام جريمة التزوير، بل لا بد من أن تتجه إرادته إلى القيام بالركن المادي المكون لجريمة التزوير.

2- القصد الجنائي الخاص المتمثل في جريمة التزوير باتجاه نية الجاني إلى استعمال المحرر فيما زور من أجله حتى ولو لم يستعمله[3].

وإذا انتفت هذه النية انتفى القصد الجنائي، وتطبيقاً لذلك لا يسأل عن جريمة التزوير مثلاً من يصطنع سنداً بدين على شخص معين ويوقع عليه بإمضاء هذا الشخص

---

(1) المصدر السابق، ص 91.

(2) عفيفي، مرجع سابق، ص 238.

(3) انظر، السعيد، شرح قانون العقوبات...مرجع سابق، ص 125 وما بعدها.

متى ثبت انه لم يقصد بذلك سوى اختبار قدرته على التقليد وأن نيته كانت متجهة إلى إعدام المحرر في الحال[1].

المطلب الثاني: مدى انطباق أركان جريمة التزوير التقليدية في قانون العقوبات الأردني على التزوير المعلوماتي

287 ـ التزوير المعلوماتي الذي يقع على المعلومات أو البيانات والمعطيات التي يحتويها النظام المعلوماتي قد يتخذ عادة إحدى الصور التالية:

الصورة الأولى:

تتمثل في التلاعب بالمعلومات داخل النظام المعلوماتي لتغيير الحقيقة فيها. وهذا التلاعب قد يتم عن طريق تعديل هذه المعلومات أو من خلال محو جزء أو عدة أجزاء منها.

وعملية تعديل المعلومات والمعطيات تقنية سهلة و شائعة من تقنيات الإجرام المعلوماتي، وهي تتمثل في تعديل المعلومات أو المعطيات قبل أو أثناء إدخالها إلى النظام المعلوماتي أو في لحظة إخراجها منه[2].

أما الوجه الآخر للتلاعب بالمعلومات والمتمثل في محو جزء أو عدة أجزاء منها، فيمكن الإشارة إلى ما قام به القائمون على أحد المراكز الطبية في ألمانيا، حيث تمكنوا من اختلاس مبلغ (61.000) دولار وهي عبارة عن مبالغ مدفوعة مرسلة من شركات التأمين للمركز الطبي. وحتى تتم هذه العملية بنجاح قام هؤلاء الأشخاص بمحو الحسابات الموجودة في جهاز الحاسوب الخاص بالمركز لجعلها غير قابلة للتحصيل[3].

---

(1) الصغير، مرجع سابق، ص 178.

(2) محمود، مرجع سابق، ص 101.

(3) الصغير، مرجع سابق، ص 45، 44.

الصورة الثانية:

تتمثل هذه الصورة في إدخال معلومات غير صحيحة إلى النظام المعلوماتي، أو بمعنى آخر إدخال معلومات مصطنعة.

وعملية إدخال المعلومات غير الصحيحة أو المصطنعة إلى النظام المعلوماتي يمكن أن تتم على سبيل المثال من خلال ضم مستخدمين غير موجودين بالفعل إلى إحدى المنشآت أو المؤسسات. ويكون ذلك عادة في المنشآت التي تضم العديد من الفروع التي يتغير عدد مستخدميها وفقاً للظروف الاقتصادية، حيث يمكن أن يقدم مدير أحد هذه الفروع معلومات وهمية إلى الإدارة المركزية تفيد استئجار مستخدمين مؤقتين، ويقوم هذا المدير بعد ذلك باستلام الشيكات النقدية الخاصة بالمستخدمين المؤقتين المزعومين[1].

288 ـ أما فيما يتعلق بمدى انطباق نصوص جريمة التزوير التقليدية في قانون العقوبات الأردني على التزوير المعلوماتي، فنحن نرى أنه من الصعوبة بمكان مد نصوص قانون العقوبات المتعلقة بجريمة التزوير لتشمل هذا النمط المستحدث من الجرائم المعلوماتية.

289 ـ فالتزوير استناداً إلى قانون العقوبات لا بد أن يقع في محرر مكتوب، والمحرر ـ كما سبق وأشرنا ـ هو كل مسطور يتضمن علامات ينتقل بها الفكر لدى النظر إليها من شخص إلى آخر، وبالتالي لا يمكن تطبيق النصوص المتعلقة بالتزوير على تغيير الحقيقة الذي يطرأ على المعلومات المعالجة آليا ـ قبل أن تتخذ شكل المحرر الالكتروني ـ حيث إنها لا تعتبر محرراً مكتوباً. كذلك هو الحال بالنسبة للمعلومات المسجلة كهرومغناطيسياً على وسائط التخزين الخاصة بها إذ لا يمكن مشاهدة هذه المعلومات عن طريق النظر المباشر[2]. فهذه المعلومات مخزنة في ذاكرة الحاسوب أو في الأقراص الممغنطة أو المدمجة أو على أية دعامة مادية ليست مقروءة ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين المجردة وبالتالي فإنها تفتقر إلى صفة المحرر.

---

(1) الشوا، ثورة المعلومات... مرجع سابق، ص 72.

(2) قورة، مرجع سابق، ص 603، 602.

290 ـ أما مستخرجات الحاسوب من المحررات أو المستندات المعلوماتية (الالكترونية) فإنها تكون مشمولة بالنص الخاص بجريمة التزوير في قانون العقوبات، خاصة أنها أصبحت تتمتع في التشريع الأردني بقوة الإسناد العادية في الإثبات[1].

291 ـ وقد كان هناك جانب من الفقه[2] تحديداً من الفقه الفرنسي، يذهب إلى إمكانية تطبيق نصوص التزوير التقليدية على التزوير المعلوماتي، مستندين في ذلك إلى أن الكتابة إن كانت مطلباً تقليدياً في جرائم تزوير المحررات إلا أنه بالإمكان تغليب روح النصوص على الألفاظ واعتبار ما يظهر على شاشة الحاسوب شكل مستحدث للمحرر.

كما ذهب هذا الاتجاه أيضا إلى أنه بالرغم من أن وجود محرر هو شرط مفترض في جريمة التزوير، إلا أن القضاء لا يفرق بين محرر منسوخ أو مختزل (أي مشفر وفقاً للغة المعلوماتية). [3].

292 ـ إلا أن المشرع الفرنسي قد حسم الجدل في قانون العقوبات الفرنسي لسنة 1992 والمعمول به منذ عام 1994 وذلك في المادة (1/441) منه التي توسعت في مفهوم المحرر الذي يقع عليه التزوير حيث أصبحت تشمل إلى جانب المحرر بشكله التقليدي كل وسيط آخر للتعبير عن فكرة. ويشمل ذلك بطبيعة الحال الأقراص المغنطة والاسطوانات المدمجة وغيرها من وسائط تخزين المعلومات. ويشترط القانون أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف أو أن يصلح لإثبات حق أو تصرف له آثار قانونية.

---

(1) الشوابكة، مرجع سابق، ص 233. وتنص المادة (13) من قانون البنيات رقم (37) لسنة (2001) في فقرتها الثالثة على ما يلي:

أ- " تكون لرسائل الفاكس والتلكس والبريد الالكتروني قوة الإسناد العادية في الإثبات ما لم يثبت من نسب اليه إرسالها انه لم يقم بذلك أو لم يكلف احداً بإرسالها.

ب- وتكون رسائل التلكس بالرقم السري المتفق عليه بين المرسل او المرسل اليه حجة على كل منهما.

ج- وتكون لمخرجات الحاسوب المصدقة أو الموقعة قوة الاسناد العادية من حيث الاثبات ما لم يثبت من نسب اليه انه لم يستخرجها او لم يكلف احداً باستخراجها ".

(2) انظر، عفيفي، مرجع سابق، ص 225.

(3) الشوا، ثورة المعلومات... مرجع سابق، ص 159.

293 ـ وفي كندا ، شمل تعديل قانون العقوبات عام 1985 تعريف المحررات في جريمة التزوير ليشمل أي شيء مادي يمكن أن يتم عليه تسجيل معلومات يمكن قراءتها أو فهمها بواسطة أي شخص أو بواسطة أنظمة الحواسيب أو بواسطة أي جهاز آخر[1].

294 ـ وفي استراليا ، فإن قانون العقوبات الخاص بالكومنولث الاسترالي ينص على أنه يعد مرتكباً لجريمة التزوير كل من يقوم بتزوير محرر أو توقيع أو تسجيلات. ويتسع لفظ تسجيلات ليشمل المعلومات المسجلة الكترونياً. و منذ عام 1986 بمقتضى التعديل الذي طرأ على قانون العقوبات يعد مرتكباً لجريمة التزوير كل من يقوم بخلق أو استخدام أداة مزورة أو نسخة من هذه الأداة بنية إقناع شخص آخر بقبولها بوصفها أداة حقيقية للقيام أو للامتناع عن العمل.

ويعرف القانون الاسترالي هذه الأداة بأنها كل محرر رسميا كان أم عرفيا كذلك البطاقات الائتمانية ، والاسطوانة المدمجة أو الأقراص المغنطة والشريط الصوتي وأي جهاز آخر سجلت أو حفظت فيه أو عليه أية معلومات بوسائل ميكانيكية أو وسائل أخرى[2].

295 ـ أما قانون العقوبات الألماني لسنة 1986 فقد ورد فيه نص خاص يجرم التزوير في بيانات ذات أهمية قانونية. فلم يتطلب المشرع الألماني الإدراك البصري للمستند ، وقرر عقوبة الحبس لمدة لا تزيد على خمس سنوات أو الغرامة على كل من يقوم بقصد التحايل على الروابط القانونية بتخزين أو تغيير بيانات إذا استنسخت بهذا الشكل أنتجت مستنداً غير أصلي أو مزور[3].

296 ـ أما فيما يتعلق بالتشريع الهولندي والنرويجي والسويدي ، فلقد اعتبرت جميعها المحررات الالكترونية مساوية للمحررات في مفهومها التقليدي متى كان من الممكن قراءتها عن طريق الأجهزة الإلكترونية اللازمة لذلك[4].

---

(1) المادة (321) من قانون العقوبات الكندي لسنة 1985. انظر ، قورة ، مرجع سابق ، ص610.

(2) انظر ، قورة ، مرجع سابق ، ص 609.

(3) انظر ، عفيفي ، مرجع سابق ، ص 231 ، وكذلك ، الشوا ، ثورة المعلومات... مرجع سابق ، ص 165 ، 164.

(4) قورة ، مرجع سابق ، ص 279.

297 ـ وتجدر الإشارة إلى أن توصية المجلس الأوروبي الخاصة بجرائم المعلوماتية تضمنت الإشارة إلى جريمة التزوير المعلوماتي، واقترحت التوصية على الدول الأعضاء نموذجاً تشريعياً يتم بمقتضاه تجريم كل إدخال أو تعديل و محو أو إعاقة لمعلومات داخل الأنظمة المعلوماتية حيث يشكل هذا السلوك تزويراً وفقاً لقوانين الدولة.

وقد أشارت التوصية إلى أن الحماية الجنائية يجب أن تمتد إذا تمت طباعة هذه المعلومات لاستعمالها فيما زورت من أجله أو ظلت داخل الحاسوب لاستخدامها مباشرة بين الأنظمة المعلوماتية[1].

298 ـ وأمام قصور النصوص الجزائية في قانون العقوبات الأردني والمتعلقة بالتزوير عن شمول هذا النمط المستحدث من الجرائم المعلوماتية لا بد من تدخل المشرع الجزائي الأردني لتجريم التزوير المعلوماتي والعقاب عليه إما بتعديل نصوص جريمة التزوير القائمة أو باستحداث نص مستقل يجرم التزوير المعلوماتي صراحة و يوسع من مفهوم المحرر ليشمل كل وسيط للتعبير عن فكرة كما هو الحال في وسائط تخزين المعلومات المختلفة.

(1) المصدر السابق، ص 278.

الفصل الثالث

الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

الفصل الثالث
الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

299 ـ في هذه الحالة نكون أمام جرائم معلوماتية أداة ارتكابها الأساسية ووسيلتها هو النظام المعلوماتي[1].

ومن الصعب حصر جميع الجرائم المعلوماتية التي قد تقع تحت هذه الطائفة إلاّ أنني سأتناول بعض صور هذه الجرائم المعلوماتية في أربعة مباحث متتالية على النحو الآتي:

المبحث الأول: الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي.

المبحث الثاني: الاعتداء على حرمة الحياة الخاصة للأفراد.

المبحث الثالث: الاحتيال المعلوماتي.

المبحث الرابع: التجسس المعلوماتي.

---

(1) من القائلين بهذا التقسيم، رستم، هشام محمد فريد، (1995). جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، العدد السابع عشر، ص 9، 10.

المبحث الاول
الدخول والبقاء غير المصرح بهما الى النظام المعلوماتي

300 ـ يتعرض النظام المعلوماتي إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول اليه أو البقاء فيه[1]، وقد ساهم في انتشار هذه الظاهرة تطور الاتصالات وتنامي شبكات المعلوماتية.

301 ـ وبالرغم من أن الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي يعد مرحلة سابقة وضرورية لارتكاب الجرائم المعلوماتية الأخرى، مثل سرقة المعلومات وتزويرها أو التجسس المعلوماتي أو جريمة الاحتيال المعلوماتي أو الاعتداء على حرمة الحياة الخاصة وغير ذلك من الجرائم، إلاّ أن مرتكب هذا الفعل قد يقصده بحد ذاته دون أن يهدف إلى ارتكاب جريمة أخرى من ورائه[2]. وقد أثارت هذه الحالة خلافاً في الفقه حول مدى انطباق وصف الجريمة المعلوماتية عليها، وبالتالي إذا كانت تستوجب الحماية الجنائية ام لا، وكان هذا الخلاف في اتجاهين :

الاتجاه الاول:

302 ـ يرى أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي، وخاصة إذا لم يكن لدى الفاعل نية لارتكاب جريمة لاحقة على هذا الدخول أو البقاء.

---

(1) يذهب د. احمد تمام إلى تصنيف هذه الجريمة تحت باب الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي. انظر، تمام، مرجع سابق، ص 259 وما بعدها.

بينما يطلق د. عبد الفتاح حجازي على هذا النموذج للسلوك الإجرامي (جرائم الاعتداء على نظم المعالجة الآلية للبيانات)، انظر حجازي، الدليل الجنائي ... مرجع سابق، ص 235.

بينما يطلق د. عمر الحسيني عليها مصطلح (جرائم السلوك المجرد المتصلة بنظام المعالجة الآلية للمعلومات) انظر، الحسيني. مرجع سابق، ص 122 وما بعدها .

(2) قورة، مرجع سابق، ص 323.

ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات التقنية والذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل وهذا الامر لا يشكل بحد ذاته جريمة تستدعي معاقبة الفاعل.

الاتجاه الثاني:

303 ـ يذهب إلى ضرورة تجريم الدخول والبقاء غير المصرح بهما الى النظام المعلوماتي، حتى لو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد.

304 ـ ويعزز هذا الاتجاه رأيه بالاشارة إلى أن هناك خسائر مادية قد تترتب على حالات الدخول غير المصرح به الى النظام المعلوماتي، وقد تكون هذه الخسائر نتيجة مجرد محاولة وقف هذا الدخول. ويمكن الإشارة في هذا الصدد إلى الخسارة التي تحملها إحدى المعامل الخاصة بتصنيع الأسلحة النووية في كاليفورنيا في الولايات المتحدة الأمريكية التي قدرت بحوالي مائة الف دولار امريكي، وهي تكلفة الأبحاث التي أُجريت لمحاولة وقف الدخول غير المصرح به الذي قام به أحد الاشخاص إلى نظام الحاسوب الخاص بهذا المعمل[1].

305 ـ ونحن من جانبنا نؤيد الاتجاه الثاني الداعي الى تجريم هذا الفعل بحد ذاته لأنه يعد مرحلة اساسية لارتكاب بقية الجرائم المعلوماتية الأخرى، كما أن المعلومات التي قد يقع عليها هذا السلوك تكون معلومات على قدر من الاهمية، كما هو الحال بالمعلومات المتعلقة بالأسرار العسكرية للدولة وكذلك البيانات الخاصة بالعملاء في البنوك أو البيانات الخاصة بالمواطنين في السجلات المدنية، وقد يطال هذا السلوك الأبحاث العلمية أو الطبية وغير ذلك من المعلومات المختلفة؛ إذ أن مجرد الدخول أو البقاء في النظام المعلوماتي والاطلاع على المعلومات التي يحويها يعد مساساً بها حتى لو لم يتم ارتكاب جريمة لاحقة على هذا الفعل، أو حتى لو كان الهدف من هذا الفعل هو مجرد إثبات الذات، والقدرات التقنية والقدرة على اختراق الحواجز الالكترونية

(1) مشار لهذه الواقعة عند قورة، مرجع سابق، ص 327، 328.

للنظـام المعلومـاتي، حيـث أن تـرك هـؤلاء الاشـخاص دون عقـاب يـؤدي إلى التمـادي في الاعتداء على الأنظمة المعلوماتية.

وسـوف نقـوم بتنـاول الـدخول غيـر المـصرح بـه الى النظـام المعلومـاتي في (المطلـب الأول)، وفي (المطلب الثاني) سنتناول البقاء غير المصرح به في النظام المعلومـاتي، حيـث يتفق الفقه[1] على أن الركن المادي يختلف في هذين الفعلين.

المطلب الأول: الدخول غير المصرح به الى النظام المعلوماتي

306 ـ تقـوم هـذه الجريمـة بتحقـق فعـل الـدخول إلى النظـام المعلومـاتي. ومـدلول كلمة الدخول تشير الى كل الأفعال التي تسمح بالولوج إلى نظام معلومـاتي والإحاطـة أو السيطرة على المعطيات والمعلومات التي يتكون منها[2].

307 ـ وفعل الـدخول الـذي يشكل الـركن المـادي في هـذه الجريمـة لا يقـصد بـه الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامـه، بل يقـصد بـه الـدخول باسـتخدام الوسـائل الفنيـة والتقنيـة إلى النظـام المعلومـاتي أي الـدخول المعنـوي أو الالكتروني.

ويتساوى في هذا المجال إن تم هذا الدخول بطريق مباشـر إلى المعلومـات أو تمّ عـن طريق الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام المعلوماتي[3].

---

(1) انظر، الحسيني، مرجع سابق، ص 126- 130، وتمام، مرجع سابق، ص 262، وكذلك قورة، مرجع سابق، ص 331، 358.

(2) قورة، مرجع سابق، ص 343.

(3) عملية الدخول إلى النظام المعلوماتي قد لا تتطلب سوى تشغيل جهاز الحاسوب، وفي بعض الأحيان يتطلب ذلك اموراً اكثر تعقيداً كما هو الحال بمحاولة الحصول على الرقم السري حتى يكون بالإمكان الدخول الى النظام، وقد يتم ذلك احيانا أخرى باستخدام برامج خبيثة يتم دمجها في أحد البرامج الأصلية لجهاز الحاسوب حيث تعمل كجزء منه وتقوم هذه البرامج بتسجيل الشيفرات التي يستخدمها المستخدمون الشرعيون للدخول إلى النظام واستعمالها بعد ذلك لاختراق النظام المعلوماتي. وهناك وسائل تعتمد على ضعف الأنظمة ذاتها أو على الاخطاء الناجمة عن عملية البرمجة، ووسائل الدخول غير المصرح به من الصعب حصرها لأنها تعتمد على التطور التقني في مجال المعلوماتية. انظر المصدر السابق، ص 325.

308 ـ وفعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكاً غير مشروع، وإنما يتخذ هذا الفعل وصفه الجرمي انطلاقا من كونه قد تم دون وجه حق، أو بمعنى آخر دون تصريح، ومن الحالات التي يكون فيها الدخول غير مصرح به إلى النظام المعلوماتي:

دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح من المسؤول عن النظام أو مالكه، وقد يكون الفاعل مصرحاً له بالدخول الى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويدخل إلى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول إليها، وهذا الفرض يتم في الغالب من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي.

كما أن عدم التصريح بالدخول ينصرف إلى الحالات التي يكون فيها هذا الدخول مشروطاً بدفع ثمن محدد وبالرغم من ذلك يدخل الفاعل إلى النظام دون أن يقوم بتسديد هذا الثمن، أما إذا كان الولوج إلى النظام المعلوماتي بالمجان وكان متاحاً للجمهور، ففي هذه الحالة يكون الدخول إليه حقاً من الحقوق[1].

309 ـ تعد جريمة الدخول غير المصرح به إلى النظام المعلوماتي من الجرائم الشكلية التي لا يتطلب قيام الركن المادي فيها نتيجة ما. وبالرغم من إمكانية حدوث أضرار معينة بالمعلومات بمحوها أو بتعديلها أو إفساد نظام التشغيل نتيجة عملية الدخول غير المصرح به، إلاّ أن ذلك لا يغير من طبيعة الجريمة باعتبارها جريمة شكلية[2].

310 ـ قد حدث خلاف في الفقه حول مدى أحقية النظم المعلوماتية التي لا تحميها نظم أمنية معينة بالحماية الجنائية ضد الدخول غير المصرح به. وقد كان هناك اتجاهان:

الاتجاه الاول:

311 ـ يرى أنه من غير المعقول توفير الحماية الجنائية لمعلومات على درجة من الأهمية، تركت دون أية اجراءات أمنية تكفل لها الحماية اللازمة.

---

(1) احمد، الجوانب الموضوعية ... مرجع سابق، ص 72، 73.

(2) الصغير، مرجع سابق، ص 150. وكذلك، الحسيني، مرجع سابق، ص 128.

ويعزز اصحاب هذا الرأي وجهة نظرهم بالإشارة إلى أن القانون الجنائي لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم والمطلوب من الانسان متوسط الذكاء فوجود نظام حماية يمكن اعتباره التزاماً مفروضاً على كل من يقوم بإدارة نظام معلوماتي[1].

الاتجاه الثاني:

312 ـ يرى ـ وهو الاتجاه الذي نؤيده ـ أنه ينبغي حماية الأنظمة المعلوماتية سواء أكانت هناك تدابير أمنية تحيط بها و تحميها أم لم تكن.

ويعزز هذا الاتجاه وجهة نظره بالإشارة إلى أن تطلب هذا الشرط يؤدي الى قصر نطاق الحماية على الأنظمة المحمية فقط دون الأنظمة المفتوحة للجمهور مثل الدليل الالكتروني[2] مما يعني توسيع دائرة الافلات من العقاب.

كما يذهب أنصار هذا الرأي إلى أنه لا ينبغي أن ينظر إلى الأنظمة الأمنية باعتبارها شرطاً لتجريم الدخول غير المصرح به إلى النظام المعلوماتي وإنما يمكن النظر اليها باعتبارها قرينة على تحقق القصد الجنائي[3].

313 ـ وتجدر الاشارة إلى أن اكتمال عناصر جريمة الدخول غير المصرح به إلى النظام المعلوماتي تستدعي توافر القصد الجنائي العام والمتمثل في عنصري العلم والارادة.

فالفاعل لا بد أن يعلم أنه يقوم بفعل الدخول غير المصرح به إلى النظام المعلوماتي، ولا بد كذلك من ان تكون إرادته متجهة لارتكاب هذا الفعل.

ويتعين أن يكون القصد الجنائي معاصراً للنشاط الإجرامي، بمعنى أن تخلف القصد لحظة بدء فعل الدخول غير المصرح به ينفي الصفة الاجرامية عن هذا الفعل[4].

---

(1) انظر، تمام، مرجع سابق، ص 260.

(2) الصغير، مرجع سابق، ص 151.

(3) انظر، قورة، مرجع سابق، ص 371.

(4) الحسيني، مرجع سابق، ص 129.

المطلب الثاني: البقاء غير المصرح به في النظام المعلوماتي

314 ـ يقصد بفعل البقاء غير المشروع داخل النظام المعلوماتي هو التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه[1].

315 ـ ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل لنظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة إلاّ أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به.

فالركن المادي في هذه الحالة لا يتمثل في إقامة الاتصال مع النظام، فالفرض هنا أن هذا الاتصال لم يقصده ولم يرده الجاني[2]. ويمكن تصور ذلك في الحالة التي يكون فيها الشخص في سبيله للدخول إلى نظام معلوماتي له الحق في الدخول إليه، إلاّ أنه يجد نفسه ولسبب ما ـ مثل استخدام شيفرة خاطئة مثلا ـ داخل نظام آخر.

316 ـ وتعتبر جريمة البقاء غير المشروع داخل النظام المعلوماتي بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها، حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه[3].

317 ـ وتعد هذه الجريمة كذلك من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة جرمية معينة، فيكفي البقاء غير المصرح به داخل النظام المعلوماتي ليقوم الركن المادي لهذه الجريمة.

318 ـ وجريمة البقاء غير المشروع داخل نظام معلوماتي تعتبر من الجرائم المستمرة[4] وذلك نظراً لاستمرار الاعتداء على المصلحة التي يحميها القانون طالما استمر البقاء غير المصرح به داخل النظام.

---

(1) حجازي، الدليل الجنائي ... مرجع سابق، ص 235.

(2) الحسيني، مرجع سابق، ص 105.

(3) الشوا، ثورة المعلومات ... مرجع سابق، ص 210.

(4) الجريمة المستمرة هي " الجرمية التي يتكون ركنها المادي من تصرف او حالة تحتمل بطبيعتها الاستمرار لفترة زمنية غير محددة من الوقت." انظر، صالح، محاضرات في قانون العقوبات ... مرجع سابق، ص 46 .

وتجدر الإشارة إلى أن جريمة الدخول غير المصرح به الى نظام معلوماتي تعد من الجرائم الوقتية[1] حيث أن هذه الجريمة تتم بمجرد تحقق فعل الدخول غير المصرح به.

وتجدر الإشارة إلى أنه في الحالة التي يتم فيها الدخول غير المصرح به إلى النظام المعلوماتي ومن ثم البقاء فيه فترة من الزمن يتحقق الاجتماع المادي للجرائم[2].

319 ـ ومما لا شك فيه أن جريمة البقاء غير المصرح به داخل النظام المعلوماتي تعتبر جريمة عمدية، يستلزم قيامها توافر القصد الجنائي العام والمتمثل في عنصري العلم والإرادة. أولاً علم الجاني بأنه يقوم بالتجول داخل نظام معلوماتي من غير المصرح له البقاء فيه، واتجاه إرادته في ذات الوقت إلى البقاء فيه وعدم قطع الاتصال مع هذا النظام.

320 ـ وفي الواقع فإن قانون العقوبات الأردني لا يوجد فيه أي نص يجرم هذا السلوك ـ كما هو الحال تماما بالنسبة لباقي الجرائم المعلوماتية ـ ولا بد للمشرع الجزائي الاردني من التدخل لتجريم هذا الفعل بنص صريح.

321 ـ ونشير في هذا المجال إلى ما نصت عليه اتفاقية بودابست لمكافحة الإجرام المعلوماتي في المادة الثانية منها، حيث جاء فيها (يجب على كل طرف في الاتفاقية ان يتبني الاجراءات التشريعية أو أية إجراءات يرى أنها ضرورية من أجل اعتبار جريمة جنائية الولوج العمدي لكل أو لجزء من جهاز الحاسوب دون حق، كما يمكن أن تشترط التشريعات أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن)[3].

322 ـ من الدول العربية التي جرمت الدخول والبقاء غير المشروع في النظام المعلوماتي بنصوص صريحة دولة سلطنة عُمان، التي نص قانون العقوبات فيها على أنه (يعاقب بالسجن مدة لا تقل عن ثلاثة اشهر ولا تزيد عن سنتين وبغرامة (1000) ريال

---

(1) الجريمة الوقتية هي " الجريمة التي يتكون ركنها المادي من تصرف يقع في وقت محدود، اي فترة زمنية قصيرة وتنتهي بوقوع الجريمة." انظر، المصدر السابق، ص 45.

وتجدر الاشارة إلى أن د. جميل الصغير يرى أن جريمتي الدخول والبقاء غير المصرح بهما داخل النظام المعلوماتي تعتبر من الجرائم المستمرة. انظر في ذلك: الصغير، مرجع سابق، ص 150.

(2) انظر، الشوابكة، مرجع سابق، ص 25، 26.

(3) مشار إلى هذه المادة عند أحمد، الجوانب الموضوعية والإجرائية ... مرجع سابق، ص 68.

إلى (5000) ريال او بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسوب في ارتكاب أحد الأفعال الآتية:

1- الالتقاط غير المشروع للبيانات.

2- الدخول غير المشروع الى أنظمة الحاسوب.....)[1].

وقد نص كلا من القانونين الانجليزي[2] والأمريكي[3] بشكل صريح على تجريم هذا الفعل.

323 ـ أمّا المشرع الجزائي الفرنسي فلقد نص في قانون العقوبات الفرنسي في المادة 1/323 على ما يلي:

(كل شخص قام بالدخول، أو البقاء كلياً أو جزئياً في داخل نظام لمعالجة المعلومات يعاقب بالحبس لمدة سنة وبغرامة مالية قدرها (15000) يورو، واذا نجم عن هذا الدخول غير المشروع محو أو تعديل في المعلومات الموجودة داخل النظام أو نجم عن هذا الدخول إتلاف تشغيله تكون العقوبة الحبس سنتين وثلاثمائة ألف يورو غرامة).

ونلاحظ أن المشرع الفرنسي قد جرم مجرد الدخول أو البقاء غير المشروع داخل النظام المعلوماتي حتى لو لم ينجم عن هذا الفعل ضرر يذكر بالنظام المعلوماتي، وشدد العقوبة في حالة أن نجم عن هذا السلوك محو أو تعديل أو إتلاف للمعلومات.

---

(1) المرسوم السلطاني 72/2001 حول تعديل بعض احكام قانون الجزاء العُماني. انظر، الرومي، مرجع سابق، ص7.

(2) اصدر المشرع الانجليزي قانون إساءة استخدام الحاسوب لعام 1990، وقد نصت المادة الأولى منه على تجريم فعل الدخول غير المشروع الى النظام المعلوماتي.

(3) اصدر المشرع الأمريكي قانون الاحتيال وإساءة استخدام الحاسوب لعام 1996 والذي جرم كذلك فعل الدخول غير المشروع الى نظام معلوماتي.

المبحث الثاني
الاعتداء على حرمة الحياة الخاصة للأفراد

324 ـ الحق في احترام الحياة الخاصة (الخصوصية)[1] هو أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه انساناً. وفي المجتمعات الحديثة يعتبر هذا الحق من أهم الحقوق؛ وذلك لما له من ارتباط وثيق بحرية الفرد.

325 ـ إلاّ أن المعلوماتية بأدواتها المتمثلة في جهاز الحاسوب والشبكات العالمية والمحلية للمعلومات وما لهذه الأأوات من قدرة فائقة على جمع أكبر قدر من المعلومات والبيانات الاسمية واسترجاعها وتصنيفها وتحليلها ومعالجتها ومن ثم تبادلها دون أي عوائق بين الجهات المختلفة كل ذلك يشكل تهديداً حقيقياً لحق الأفراد في احترام حياتهم الخاصة.

فحياة الشخص التي كان يكسوها في الماضي ظلال كثيفة لا تسمح لأي فرد بالكشف عنها، أصبحت الآن أمام تكنولوجيا المعلومات شفافة واضحة، وأصبح بالإمكان ترجمة حياة الفرد في أقل من الثانية الواحدة[2] خاصة مع انتشار ما يسمى ببنوك المعلومات.

326 ـ ولقد لخص "آرثر ملير" المخاطر المتولدة عن استخدام الأنظمة المعلوماتية على الحياة الخاصة للأفراد بقوله[3]:

(إن الحاسوب بشراهته التي لا تشبع في جمعه للمعلومات، وما هو معروف عنه من دقة وعدم نسيان أي شيء يوضع فيه، قد تنقلب معه الحياة رأساً على عقب.

(1) الحق في الحياة الخاصة هو المصطلح الذي يستخدمه الفقه في النظم اللاتينية، في الوقت الذي يستخدم الفقه في النظم الانجلوسكونية مصطلح الخصوصية.

(2) قايد، أسامة عبدالله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، بدون ناشر، 1988، ص6.

(3) انظر، بحر، ممدوح خليل، حماية الحياة الخاصة في القانون الجنائي، ط1، دار النهضة العربية، القاهرة، 1983، ص16.

فيخضع الأفراد لنظام رقابي مشدد يتحول معه المجتمع إلى عالم شفاف ترقد فيه مكشوفة بيوت الناس ومعاملاتهم المالية وحالتهم العقلية والجسمانية لأي مشاهد).

327 ـ ومن هنا كان لا بدّ من التصدي للإجرام المعلوماتي الذي قد يطال حقاً من أهم حقوق الإنسان ألا وهو الحق في الحياة الخاصة.

وللوقوف على هذا الموضوع أتناول في (المطلب الأول) الحياة الخاصة في مواجهة المعلوماتية، ثم أعرض لأهم صور التهديد المعلوماتي للحق في الخصوصية في (المطلب الثاني)، أما (المطلب الثالث) والأخير فأخصصه لمدى توافر الحماية الجنائية للحق في الحياة الخاصة في قانون العقوبات الأردني من الجرائم المعلوماتية التي قد تقع عليها.

المطلب الأول: الحياة الخاصة في مواجهة المعلوماتية

328 ـ ابتداء لا بدّ أن أشير إلى أن تعريف الحياة الخاصة أمر لا يخلو من الصعوبة و هذا ما يقرره الفقه؛ نظراً لاختلاف نطاق الخصوصية من فرد لآخر. فهناك من يجعل حياته الخاصة كتاباً مفتوحاً وهناك من يجعل حياته الخاصة سراً غامضاً. كما يختلف مضمون الحياة الخاصة من مجتمع لآخر نتيجة لاختلاف القيم الأخلاقية والتقاليد والثقافة، ولكن يجب التأكيد على أن الخلاف ينصب على نطاق الحق في الحياة الخاصة لكنه لا يمتد إلى الحق في الخصوصية فهو حقيقة مؤكدة لجميع الأفراد في كل المجتمعات[1].

329 ـ توجد في الحقيقة تعريفات متعددة ومتنوعة في الفقه قيلت بشأن الحق في الحياة الخاصة، فقد عرفه البعض أنه: (الحق الذي يكون للأفراد والجماعات والهيئات والمؤسسات في أن يحددوا لأنفسهم متى وكيف وبأي قدر يمكن إيصال المعلومات الخاصة بهم إلى غيرهم)[2].

---

(1) قايد، مرجع سابق، ص 9.

(2) تعريف الفقيه الامريكي (Allen westin). مشار له عند، بحر، مرجع سابق، ص168.

وقد ذهب البعض الآخر[1] الى أن الحق في الحياة الخاصة والحقوق الشخصية يكادان يكونان متطابقين لأنهما يقرران حق الفرد في حماية اسمه ومراسلاته واتصالاته وشرفه واعتباره وحياته المهنية والعائلية وكل ما له تأثير على حياته الشخصية.

أما مؤتمر استكهولم لرجال القانون الذي عقد في عام 1967 فقد تبنى تعريفاً مقارباً للتعريفات السابقة حيث عرّفه أنه: (الحق في أن يكون الفرد حراً وأن يترك ليعيش كما يريد مع أدنى حق للتدخل الخارجي)[2].

330 ـ جانب آخر من الفقه ذهب إلى تعريف الحق في الحياة الخاصة تعريفاً سلبياً بالإشارة إلى أنه كل ما لا يعتبر من قبيل الحياة العامة للشخص.

331 ـ وفي الواقع فإن معظم الفقهاء الذين تناولوا تعريف الحق في الحياة الخاصة يجمعون على أنه من الصعوبة إن لم يكن من المستحيل إعطاء فكرة قانونية عامة لمفهوم الحق في الخصوصية، فهناك ازدواج في حياة الإنسان العامة والخاصة[3].

332 ـ ولهذا السبب اتجه الفقه تدريجياً إلى العدول عن البحث عن تعريف للحق في الحياة الخاصة واتجه إلى وضع قائمة للقيم التي تعطيها فكرة الخصوصية. وهذا ما فعله الفقهاء الفرنسيون فحاولوا وضع قائمة بالحالات والأمور التي تدخل في إطار الحياة الخاصة فذكروا الحياة العائلية، والحياة المهنية، والحق في الصورة، وكشف الضرائب، وكشف الراتب، والمرض، ومكان قضاء أوقات الفراغ، والموارد المالية، وقد أضاف البعض الآخر الحق في الاسم والحق في الشرف والاعتبار والحق في النسيان وماضي الشخص، وأضاف البعض الآخر الحياة الروحية الداخلية التي يمارسها الانسان خلف بابه المغلق[4].

(1) هذا ما ذهب اليه الفقيه الفرنسي (Ean Malherbe) . مشار له عند، قايد، مرجع سابق، ص12.

(2) انظر، المصدر السابق، ص245.

(3) بحر، مرجع سابق، ص166.

(4) لمزيد من التفاصيل راجع، بحر، مرجع سابق، ص228.

333 ـ وأمام صعوبة وضع تعريف محدد للحياة الخاصة ذهب البعض[1] إلى أنه من الأفضل أن يترك الأمر للقضاء وفقاً للتقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع بما يضمن للفرد احترام ذاتية الشخصية ويحقق له السكينة والأمان بعيداً عن تدخل الآخرين في حياته، ونحن نؤيد هذا الرأي فمن الصعب تحديد ما يعتبر من قبيل الحياة الخاصة بصورة مطلقة والأجدى أن يترك الامر للقضاء وفقاً لظروف كل قضية ووقائعها.

334 ـ وللحق في الحياة الخاصة وجهان متلازمان، هما حرية الحياة الخاصة وسرية هذه الحياة. وحرية الحياة الخاصة تعني حرية الفرد في اختيار أسلوب حياته دون تدخل من الغير أو السلطة، لكن هذه الحرية ليست مطلقة بل مقيدة بالنظام الاجتماعي داخل المجتمع ويضع القانون حدودها من أجل تنظيم كيفية ممارستها كي لا تضر بالآخرين.

أما بالنسبة لسرية الحياة الخاصة، فتعني سرية كل ما ينتج عن ممارسة الفرد لحياته الخاصة. ونطاق سرية الحياة الخاصة نطاق شخصي يرتبط بالشخص ذاته، فهو يشمل جميع البيانات والوقائع التي يقرر الشخص أن من مصلحته الاحتفاظ بها لنفسه أو لغيره من الأشخاص المتصلين به ويريد اطلاعهم عليها[2].

335 ـ والمساس بالحياة الخاصة للأفراد يزداد بشكل يبعث على القلق في ظل المجتمع المعلوماتي خاصة مع انتشار بنوك المعلومات (Data Banks).

336 ـ ويقصد بمصطلح بنك المعلومات: (قاعدة بيانات تفيد موضوعاً معيناً، وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الالكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة)[3].

(1) قايد، مرجع سابق، ص14.

(2) المصدر السابق، ص21.

(3) انظر، المصدر السابق، ص48.

وكذلك يمكن تعريفه أنه: مجموعة معلومات متعلقة بقطاع معين من المعارف ومنظمة على نحو معين يسمح بتقديم المشورة إلى العملاء[1]. وتسمح بنوك المعلومات كذلك بتقديم معلومات أو بيانات عن الأفراد بصورة تمكن من التعرف على أشخاصهم من أسمائهم أو بأي وسيلة أخرى.

337 ـ وتتعدد وتتنوع بنوك المعلومات فهناك بنوك للمعلومات الطبية أو السياسية أو الأمنية أو العسكرية، وكذلك هناك بنوك للمعلومات القانونية أو المالية. كما يمكن أن يشتمل بنك المعلومات على أكثر من نوع من أنواع البيانات السابقة، كما هو الحال في بنوك المعلومات القومية التي تتضمن قواعد بيانات عن نواحي الحياة المختلفة للافراد[2].

338 ـ وفي الواقع فإن البيانات أو المعلومات الاسمية التي يتم تجميعها ومعالجتها وتخزينها في بنوك المعلومات هي التي تمس الحق بالحياة الخاصة للأفراد، فالمعلومات قد تكون موضوعية أو ذاتية وقد تكون اسمية أو مجهولة.

والمعلومة الموضوعية هي تلك المعلومة التي لا تعكس آراء شخصية للغير، وإنما تتعلق ببيانات مجردة مثل الاسم والموطن والحالة المدنية. وتعتبر المعلومة الموضوعية من مميزات الشخصية لمن تتعلق به باعتبار أنه صاحب عناصر المعلومة[3].

339 ـ أما المعلومة الذاتية فهي تلك التي تحمل رأياً ذاتياً عن الغير، مثل تقارير كفاية العاملين[4]. والمعلومة الموضوعية أو الذاتية تتعلق عادة بالحياة العامة للأفراد.

340 ـ أما المعلومات أو البيانات الاسمية فهي البيانات التي من شانها تحديد شخصية الشخص الطبيعي بشكل مباشر أو غير مباشر، اجريت المعالجة الالكترونية عليها بواسطة شخص طبيعي أو معنوي[5].

---

(1) الغريب، مرجع سابق، ص11. ويمكن تعريف بنوك المعلومات كذلك على أنها (مجموعة المعلومات التي يتم معالجتها وذلك من أجل بثها عبر شبكة الانترنت) انظر، الاباصيري، فاروق محمد، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، ط1، دار الجامعة الجديدة للنشر، القاهرة، 2003، ص51.

(2) قايد، مرجع سابق، ص48.

(3) حسبو، مرجع سابق، ص35.

(4) المصدر السابق، ص35.

(5) هذا التعريف تبناه المشرع الفرنسي في القانون الخاص بالمعالجة الالكترونية والحريات الصادر في 6 يناير سنة 1978. مشار له عند، قايد . مرجع سابق، ص 62.

وقد تم تعريف البيانات الاسمية أنها: (البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء، كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية، عندما تكون هذه البيانات محلاً للمعالجة الآلية)[1].

341 ـ والمقصود بالمعالجة الآلية للمعلومات الاسمية: (مجموعة العمليات التي تتم آلياً، أي باستخدام الحاسوب وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات الاسمية، وكذلك مجموعة العمليات التي تتم آلياً بهدف استغلال المعلومات وعلى الأخص عمليات الربط والتقريب وانتقال المعلومات الاسمية ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومة ذات دلالة خاصة)[2].

ويقابل المعلومة الاسمية المعلومة المجهولة التي لا تدل على من تتعلق به، وبالتالي لا تثير أية صعوبة لأن المجهول لا خصوصية له.

342 ـ ويبدو أن الخطورة التي تشكلها بنوك المعلومات ونظم المعلومات بشكل عام على الحق في الحياة لخاصة لم تكن محل اتفاق الجميع. فقد حدث خلاف في الفقه حول ما إذا كانت هذه الوسائل التقنية المستحدثة تشكل خطراً حقيقياً على الحق في الخصوصية للأفراد، وقد كان هناك اتجاهان فيما يتعلق بهذا الأمر:

الاتجاه الأول:

343 ـ يذهب هذا الاتجاه[3] إلى أن الانظمة المعلوماتية لا تشكل خطراً على الحياة الخاصة للأفراد وبالتالي فلا حاجة لسن نصوص قانونية خاصة تحكم هذه المسألة.

---

(1) صالح، نائل عبد الرحمن، واقع جرائم الحاسوب في التشريع الجزائي الأردني، ورقة عمل مقدمة إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000، ص 10.

(2) هذا التعريف للمعالجة الآلية للمعلومات الاسمية كما نصت عليه المادة الخامسة من القانون الفرنسي الصادر 6 يناير سنة 1978 الخاص بالمعالجة الالكترونية والحريات. مشار له عند، حسبو، مرجع سابق، ص 50 . وقايد، مرجع سابق، ص 64.

(3) لمزيد من التفاصيل حول هذا الاتجاه أنظر، الغريب، مرجع سابق، ص 78. وحسبو، مرجع سابق، ص 55، 56.

فهذا الاتجاه لا يرى في الحاسوب إلاّ وسيلة الكترونية لتجميع المعلومات والبيانات وتخزينها ومعالجتها وهذه الوسيلة حلت محل الوسائل اليدوية كالملفات والبطاقات، وبالتالي فإن تطبيق النصوص القانونية القائمة يكفي لحماية الحياة الخاصة من أخطار بنوك المعلومات والأنظمة المعلوماتية بشكل عام، فالقضاء قادر ـ وفقا لهذا الاتجاه ـ على تطويع النصوص القانونية المتعلقة بالخصوصية على المخاطر التي قد يثيرها استخدام النظام المعلوماتي على الحياة الخاصة.

كما يرى هذا الاتجاه أن النظام المعلوماتي باعتباره مجرد آلة، يمكن إحاطته بنظام أمان يمنع تسرب المعلومات المخزنة فيه أو الاطلاع عليها أو استخدامها بشكل غير مشروع من قبل الغير.

الاتجاه الثاني:

344 ـ وهو الاتجاه الغالب ـ الذي نؤيده ـ حيث يرى أن الأنظمة المعلوماتية وخاصة بنوك المعلومات تشكل خطراً حقيقياً على الحياة الخاصة للافراد، الأمر الذي يستدعي وضع نصوص قانونية خاصة لمواجهة هذه الاخطار المستحدثة.

345 ـ وخطورة الأنظمة المعلوماتية وتحديداً بنوك المعلومات على الحق في الخصوصية يعود إلى عدة اعتبارات منها:

346 ـ إن الحاسوب يتميز بالسرعة الفائقة في العمل وسعة غير محدودة في استيعاب البيانات والمعلومات المختلفة عن الأفراد وتنظيمها وتخزينها في ذاكرته والقدرة على استرجاعها في أي وقت، الامر الذي يمكن القول معه بامكانية الاطلاع على قدر لا يستهان به من هذه البيانات التي قد تكون متكاملة و متصلة بجوانب الحياة الخاصة للفرد وذلك بمجرد جولة سريعة قد لا تستغرق اكثر من ثوان معدودة[1]، بعد أن كان من الصعب الحصول على معلومات كاملة عن حياة الأشخاص بهذه السرعة والسهولة.

---

(1) الحسيني، مرجع سابق، ص 52.

وتزداد الخطورة على الحياة الخاصة للأفراد اذا تم ربط هذه الحاسبات ببعض أو بحاسوب مركزي أو بنوع من الشبكات العامة المخصصة للاتصال على نحو يسمح بأن تتبادل هذه الحواسيب البيانات فيما بينها ، حيث يكون من شأن ذلك ان يتم ربط هذه البيانات بعضها ببعض على نحو يجعل الفرصة سانحة لاستكمالها والقيام بتحليلها ومعالجتها بصورة قد تؤدي في الكثير من الأحيان للتوصل إلى معلومات أو بيانات جديدة سواء أكانت خاصة بفرد واحد أو مجموعة من الأشخاص[1].

347 ـ وتظهر خطورة بنوك المعلومات كذلك عندما تقوم الدول بإنشاء بنوك أو مراكز للمعلومات تجمع فيها ما تشاء من البيانات عن الأفراد وتقوم بتحليلها وتنظيمها والربط بينها ومن ثم تخزينها في النظام المعلوماتي، مما يتيح للدول فرض رقابة على مواطنيها ومعرفة أدق تفاصيل حياتهم مما يشكل مساساً بحقهم في الخصوصية[2].

وقد تعالت الاحتجاجات في بعض الدول ـ كفرنسا والولايات المتحدة الامريكية والمانيا ـ ضد إنشاء النظام الموحد للمعلومات. والمقصود بهذا النظام امكانية جمع المعلومات المتصلة بالفرد في حاسوب مركزي واحد، فيمكن بالتالي جمع المعلومات الضريبية والاجتماعية والدينية والسياسية والحالة الصحية والمالية والنشاط الحزبي والنقابي لهذا الفرد حتى أوقات تسليته وفراغه والأماكن التي يرتادها.... إلخ. الأمر الذي دفع بعض الدول إلى تحريم إيجاد نظام موحد للمعلومات فيها كما هو الحال في البرتغال والنمسا[3].

348 ـ وتزداد مخاطر بنوك المعلومات على الحياة الخاصة إذا كان لكل مواطن رقم قومي[4]. حيث تتمثل خطورة هذا الرقم في تيسير الاطلاع على ما يمس الحياة

---

(1) عفيفي، مرجع سابق، ص254.

(2) في هذا الشان يقرر (Ianes Arlim) ان الحكومة الامريكية تحتفظ في الحاسبات الخاصة بها بما يوازي (3) بليون ملف تحتوي على معلومات شخصية، حيث يكون نصيب كل مواطن امريكي في المتوسط ما يقارب مائة ملف. انظر، عفيفي، مرجع سابق، ص250.

(3) منبنب، مرجع سابق، ص 163 ـ165.

(4) حسبو، مرجع سابق، ص 63، 64.

الخاصة للأفراد، فمعرفة الرقم القومي تمكن من الاطلاع على كم هائل من المعلومات المخزنة لدى الجهات المختلفة خلال لحظات.

349 ـ وإذا كان من المسلم به أن متطلبات التوجه نحو الحكومة الالكترونية تستدعي الحصول على المعلومات والبيانات الاسمية عن المواطنين وتجميعها وتخزينها في الحواسيب مع توافر امكانية تبادلها بين الدوائر الحكومية وذلك لتسهيل إنجاز المعاملات المختلفة، وإذا كانت اعتبارات المصلحة العامة والأمن القومي تتطلبان أحياناً الوقوف على تفاصيل خاصة ودقيقة في حياة الأفراد، فإن ذلك كله يستدعي في ذات الوقت ضمانات قانونية تكفل عدم المساس بالبيانات الاسمية للأفراد واستخدامها لغير الغرض الذي جمعت من أجله.

350 ـ كما إن السماح بجمع البيانات أو المعلومات عن الأشخاص مع عدم معرفة أوجه استخدامها في المستقبل يمثل أحد الأخطار التي تهدد الحياة الخاصة للافراد. وهذا الخطر لا يقتصر على البنوك العامة للمعلومات بل أيضا على البنوك الخاصة، كالبنوك التي تنشئها شركات التأمين وشركات الأموال والبنوك والمشروعات الهامة حيث تقوم بجمع بيانات تتعلق بعملائها، عن حياتهم الشخصية أو الصحية أو عن حجم معاملاتهم ومنافسيهم وغير ذلك[1]، في الوقت الذي قد تستغل فيه هذه البيانات بطريقة غير مشروعة في المستقبل.

351 ـ وتبرز خطورة الأنظمة المعلوماتية وبنوك المعلومات على الحق في الحياة الخاصة بشكل خاص من الثقة الكاملة للأفراد في نتائج المعالجة الآلية التي يستخلصها الحاسوب من المعلومات الاسمية المخزنة فيه. وتكون هذه الخطورة على الحق في الخصوصية أكثر وضوحاً اذا تمت معالجة البيانات من أجل استخلاص حكم أو تقييم للشخصية من واقع ما غذي به الحاسوب من معلومات، فمن أخطر ما يهدد الانسان استخلاص أحكام قيمية على أساس بيانات دون دراسة شخصية

---

(1) قايد، مرجع سابق، ص 58، 59 . وللتدليل على عدم الاهتمام بحرمة الحياة الخاصة نشير إلى ما حدث في الولايات المتحدة حيث قامت إحدى هيئات نظم البيانات عندما أنهت أعمالها بعرض معلوماتها عن ثلاثة ملايين مواطن للبيع مطالبة بمبلغ كبير. انظر، بحر، مرجع سابق، ص 17.

الانسان نفسه محل التقييم الأمر الذي ينتج عنه استخلاص نتائج غير دقيقة عن سلوكه أو صفاته أو سمعته مما يؤدي إلى المساس به[1].

352 ـ ولهذا تحظر المادة الثانية من القانون الفرنسي بشأن المعالجة الالكترونية والحريات أن تعتمد الأحكام القضائية أو القرارات الصادرة من السلطة الإدارية أو من الأفراد في تقديرها للسلوك البشري فقط على الدليل المستمد من المعالجة الآلية للمعلومات الاسمية[2].

وللتدليل على خطورة هذا الامر نشير إلى ما حدث عام 1965 في فرنسا عندما فصل شخص من وظيفته ومكث بعدها خمس سنوات يبحث عن عمل، لكن طلباته التي قدرت بـ (625) طلباً في مختلف الشركات والمؤسسات رفضت جميعها. وفي عام 1971 اكتشف أن الشركات والمؤسسات التي تقدم اليها عندها بطاقات قد أُعدت بواسطة شركتين تجاريتين ينحصر نشاطهما في جمع المعلومات. وقد كانت البطاقة الخاصة به تحتوى معلومات سيئة بشأنه تتعلق بشخصيته وأعماله السابقة التي كان يمارسها ومدى تقدمه في العمل من عدمه وأجره وإجازاته وأسباب الإقالة وآرائه السياسية ومعتقداته الدينية وانتماءاته النقابية[3].

المطلب الثاني: صور التهديد المعلوماتي للحياة الخاصة

353 ـ تعد الحياة الخاصة قطعة غالية من كيان الانسان لا يمكن انتزاعها منه، وإلاّ تحول إلى أداة صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وصلاته الخاصة وخصائصه المتميزة ولا يمكنه أن يتمتع بهذه الملامح إلاّ في إطار مغلق، يحفظها ويهيأ لها سبل البقاء. وتقتضي حرمة هذه الحياة أن يكون للانسان الحق في إضفاء السرية على مظاهرها[4]. وفي إطار

(1) الحسيني، مرجع سابق، ص 56. انظر كذلك، حسبو، مرجع سابق، ص 8، 9.

(2) انظر، الحسيني، مرجع سابق، ص56.

(3) مشار لهذه الواقعة عند، بحر، مرجع سابق، ص 16،17.

(4) مشار له عند، بحر، مرجع سابق، ص 192.

المعلوماتية تبرز خطورة التهديد المعلوماتي للحياة الخاصة بشكل أساسي في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد.

354 ـ وصور الاعتداء على الحياة الخاصة يصعب حصرها؛ لأنها متطورة نتيجة تطور تكنولوجيا المعلومات باستمرار. إلا أننا يمكن أن نشير إلى أبرز الانتهاكات التي قد تطال حق الأفراد في حرمة حياتهم الخاصة نتيجة لاستخدام الأنظمة المعلوماتية:

أولاً: جمع البيانات وتخزينها على نحو غير مشروع

355 ـ يتمثل فعل الانتهاك للحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني. ويستمد هذا الجمع أو التخزين صفته غير المشروعة أما من الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات والمعلومات، أو من طبيعة مضمونها.

356 ـ فمن حيث الأساليب غير المشروعة فقد يتم الاعتماد على وسائل تشكل انتهاكاً واضحاً للخصوصية وذلك من أجل جمع المعلومات والبيانات عن الأفراد. ومن ضمن هذه الأساليب القيام بالتقاط الارتجاجات التي تحدثها الأصوات في الجدران الاسمنتية للحجرات وترجمتها إلى عبارات وكلمات بواسطة حاسوب مزود ببرنامج خاص. وكذلك قد يتم مراقبة الرسائل المتبادلة واعتراضها والتقاطها عن طريق البريد الالكتروني أو توصيل أسلاك بطريقة خفية إلى الحاسوب الذي تختزن بداخله البيانات أو التوصل بطريق غير مشروع إلى ملفات بيانات تخص آخرين. أو بأي وسيلة أخرى غير مشروعة كالتدليس والغش أو التصنت على المكالمات التي تتم عن طريق شبكة الإنترنت[1].

357 ـ أما الجانب الآخر الذي يضفي صفة عدم المشروعية على جمع وتخزين البيانات هو أن تكون هذه البيانات غير صالحة للجمع والتخزين بسبب مضمونها[2].

---

(1) عفيفي، مرجع سابق، ص 258.

(2) قورة، مرجع سابق، ص 244.

وفي الواقع فإن عدم وجود ضوابط قانونية في هذا المجال قد تؤدي إلى امكانية جمع وتخزين ونقل كم كبير من المعلومات التي تتعلق بأدق التفاصيل الخاصة بالأفراد.

358 ـ فالبيانات والمعلومات الاسمية التي تتصل بالحياة الخاصة يجب أن يحظر تجميعها وتخزينها ومعالجتها داخل جهاز الحاسوب، حيث أن مضمون هذه البيانات من المفترض أنه يدخل في إطار الأمور التي يحرص الأفراد على سريتها، مع التأكيد على أن فكرة الحياة الخاصة تشتمل على قدر من المرونة، حيث تلعب إرادة الشخص دوراً في تحديد ما يدخل في إطارها[1]، فهناك أمور تدخل في نطاق الحياة الخاصة لشخص ما ولا تدخل في نطاقها بالنسبة لشخص آخر.

359 ـ كما ان المعلومات المتصلة بالجرائم والعقوبات بالنسبة للأشخاص يجب أن تكون بمنأى عن أي تجميع أو حفظ من قبل الأفراد، فلا يجوز أن يقوم بتجميع هذه المعلومات وتخزينها في الحواسيب إلاّ الجهات القضائية والسلطات العامة في الدولة وفي حدود اختصاصاتها القانونية وذلك حفاظاً على سمعة الأشخاص واعتبارهم نظراً لما لهذه المعلومات من خطورة على مستقبلهم العملي.

360 ـ كما إن المعلومات والبيانات الاسمية المتعلقة بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرقي للأفراد لا بد أن تكون بعيدة عن عمليات التجميع في الحواسيب؛ لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للافراد[2].

ثانياً: إساءة استعمال البيانات أو المعلومات الاسمية

361 ـ المعلومات والبيانات الاسمية التي يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين ان يكون لها هدف محدد وواضح ومعين سلفاً، ويشترط في هذا الهدف أو الغاية أن لا تكون متعارضة مع النظام العام والآداب.

(1) الغريب، مرجع سابق، ص 102 وكذلك، حسبو، مرجع سابق، ص 111.

(2) حسبو، مرجع سابق، ص 112، 113.

362 ـ وقد قضت المحكمة الدستورية لألمانيا الاتحادية: (أنه لا حرية رأي أو حرية اجتماع ولا حرية مؤسسات يمكن أن تمارس كاملة ما دام الفرد غير متيقن في ظل أي ظروف ولأجل أي هدف جمعت عنه المعلومات الفردية وعولجت آليا في الحاسوب)[1].

363 ـ ولا بد من التزام الجهة القائمة على النظام المعلوماتي بالهدف أو الغاية التي من أجلها قامت بتجميع المعلومات ومعالجتها الكترونياً، فلا يجوز تخزين البيانات أو المعلومات الاسمية إلا بالقدر الذي تكون مرتبطة فيه بالهدف من إقامة نظام المعالجة المقصود.

فالبيانات الاسمية يتعين أن تكون متناسبة وضرورية للهدف المقصود كما يجب أن يكون الغرض مرتبطاً بمهمة ووظيفة الجهة القائمة على النظام المعلوماتي[2].

364 ـ وتطبيقاً لذلك قضت المحاكم الالمانية بوقف إحصاء عن عدد السكان في عام 1984 بعد أن ثبت لها أن وزارة الداخلية استطاعت من خلال استمارات الإحصاء الحصول على عناوين مجموعة متطرفة إرهابية الأمر الذي يعد إساءة لاستخدام البيانات التي جمعت من أجل غاية محددة وهي الإحصاء السكاني[3].

365 ـ فإذا تم جمع المعلومات أو البيانات الاسمية لهدف محدد من قبل شخص أو جهة ما، ثم وصلت هذه المعلومات إلى شخص أو جهة أخرى تقوم بجمع معلومات لغاية أخرى، فإن تجميع هذه المعلومات إلى تلك تتيح للحائز فرصاً كبيرة وخطيرة لايقاع الضرر بالفرد. فالمشرع لا بد أن يتدخل كي يقوم بمنع أي جهة كانت عامة أو خاصة من إعطاء معلومات إلى جهة أخرى مختلفة عنها في الغاية[4]، وإذا تم هذا الامر فإنه يجب أن يكون هناك ضوابط وقيود تحكم هذه المسألة.

ثالثاً: الخطأ في المعلومات أو البيانات الاسمية

366 ـ إحدى الانتهاكات التي قد تنال الحق في الحياة الخاصة للأفراد حدوث الأخطاء التقنية أو البشرية في النظام المعلوماتي.

(1) مشار له عند، مفبفب، مرجع سابق، ص 246.

(2) حسبو، مرجع سابق، ص128.

(3) مشار له عند، قايد، مرجع سابق، ص53.

(4) مفبفب، مرجع سابق، ص 242، 243.

فالأخطاء التقنية أو الفنية من الممكن أن تقع عند تخزين المعلومات في النظام المعلوماتي ومعالجتها الكترونياً مما قد يكون له اسوأ الأثر في استخلاص نتائج معينة عن الحياة الخاصة للشخص.

367 ـ وهذه الأخطاء قد يكون مرجعها عيباً فنياً في الجهاز نفسه، أو اختلال الضغط الكهربائي الذي يترتب عليه دمج البيانات المختلفة، أو اختلال في تصنيفها وتنظيمها أو محو تسجيلها، الأمر الذي ينتج عنه نسبة معلومات معينة لأشخاص لا تتعلق بهم ويعطي صورة غير حقيقية عن حالتهم الاجتماعية أو وضعهم الحقيقي من الناحية المالية أو السياسية أو المهنية أو الصحية وكذلك التوصل إلى نتائج غير صحيحة[1].

368 ـ أما الأخطاء البشرية فيكون وقوعها عادة من قبل الاشخاص القائمين بعملية التجميع والتخزين للبيانات الاسمية وترتيبها وتصنيفها وتوزيعها، فالخطأ قد يحدث في أي مرحلة من هذه المراحل[2]. فالمعلومات التي يتم تجميعها عن فرد معين قد تكون غير صحيحة وغير دقيقة أو غير مطابقة للواقع، الأمر الذي يترك آثاراً سيئة على سيرة هذا الشخص ويلحق به أضراراً وأخطاراً كبيرة خاصة على مستقبله الوظيفي والاجتماعي، فوجود خطأ في المعلومات المتعلقة بالظروف المالية للشخص يوصد في وجهه أبواب المصارف وهيئات الائتمان، الامر الذي يعني القضاء على مستقبله المالي والاقتصادي.

رابعاً: الإفشاء غير المشروع للبيانات والمعلومات الاسمية

369 ـ من المبادئ الاساسية أن تخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أن الرضاء بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى جميع الناس[3].

(1) قايد، مرجع سابق، ص 60.

(2) المصدر السابق، ص 61.

(3) حسبو، مرجع سابق، ص 155.

370 ـ وانتهاك الحق في الحياة الخاصة قد يتخذ صورة الإفشاء غير المشروع للبيانات والمعلومات الاسمية ، فالجمع للمعلومات في هذا الفرض يكون قد تم بصورة مشروعة إلا أن هذه البيانات والمعلومات يمكن الاطلاع عليها من قبل عدد كبير من الأشخاص العاملين في حقل المعلوماتية وبالتالي قد تكون معرضة لخطر انتهاك سريتها وخصوصيتها وإفشائها للغير.

371 ـ وقد تكون المعلومات المخزنة عن الأفراد في جهاز الحاسوب أو في بنوك المعلوماتية على درجة من الحساسية والأهمية ، حيث قد يتم الحصول عليها بقصد استخدامها في ابتزاز الشخص الذي تتعلق به هذه المعلومات.

372 ـ وفي الواقع إن من شأن استخدام الانظمة المعلوماتية في المجال الأمني وقطاع الشرطة الاحتفاظ بكم هائل من المعلومات الخاصة بالملايين من الأشخاص وبالتالي فإن خطر افشائها وارد من قبل أشخاص من المفترض أنهم أمناء عليها. وللتدليل على خطورة هذا الأمر نشير إلى ما قام به ضابط شرطة نمساوي حيث قام بإعطاء أحد المخبرين الخاصين معلومات قيمة تخص بعض الأفراد متعلقة بحالتهم الجنائية والمخزنة في ذاكرة الحاسوب الذي تستخدمه الشرطة[1].

خامساً: الاعتداء على سرية الاتصالات والمراسلات

373 ـ يتفرع عن حرمة الحياة الخاصة الحق في حرمة الاتصالات والمراسلات وسريتها. فالاتصالات والمحادثات ـ أياً كان نوعها ـ التي يقوم بها الشخص تعتبر من عناصر الحق في الحياة الخاصة ، فهذه الاتصالات قد تشتمل على اسرار وخفايا يحرص الفرد على أن لا يطلع عليها أحد.

374 ـ كما إن الحق في سرية المراسلات يدخل أيضاً في إطار حق الفرد في الخصوصية. فالرسائل ـ أياً كان نوعها ـ تعتبر ترجمة مادية لافكار شخصية أو لآراء خاصة لا يجوز لغير مصدرها ومن توجه إليه الاطلاع عليها ، وفي حالة الاطلاع عليها من

(1) انظر . عفيفي. مرجع سابق، ص 259.

قبل الغير يعتبر ذلك انتهاكاً لحرمة المراسلات وبالتالي انتهاكاً للحياة الخاصة؛ لأن الرسالة قد تكون مستودعاً لسر الإنسان وخصوصياته[1].

375 ـ والحق في حماية الاتصالات والمراسلات من الاعتداء على سريتها يمتد ليشمل وسائل الاتصال الحديثة كلها التي قد تتم عن طريق النظام المعلوماتي، فالتصنت على المحادثات الخاصة التي تجري عبر شبكة الانترنت أو الاطلاع على مضمون الرسائل الالكترونية التي يتم تبادلها عبر الشبكة أيضا سواء أتمّ ذلك بالحصول على كلمة السر (Password) الخاصة بالمستخدم او باعتراض هذه الرسائل والاطلاع على مضمونها، فإن ذلك كله يعد انتهاكاً لحرمة الحياة الخاصة للأفراد الأمر الذي يستوجب العقاب والمساءلة القانونية.

376 ـ وتجدر الاشارة كذلك إلى أن التقاط الصور ونقلها يعدُّ من الانتهاكات التي قد تمس الحق في الحياة الخاصة لأن صورة الإنسان تعد من مظاهر الخصوصية التي يحظر على الغير التقاطها دون إذن صاحبها ونقلها عبر الشبكة المعلوماتية إلى الغير وتداولها بصورة غير مشروعة.

المطلب الثالث: الحماية الجنائية للحق في الحياة الخاصة في قانون العقوبات الاردني

377 ـ الحياة الخاصة للأفراد حظيت ابتداء بحماية دستورية؛ فقد كفل المشرع الدستوري الأردني الحقوق والحريات الفردية في الفصل الثاني من الدستور تحت عنوان "حقوق الاردنيين وواجباتهم".

فالحرية الشخصية كفلها الدستور في المادة السابعة حيث جاء فيها: (الحرية الشخصية مصونة). كما نصت المادة الثامنة على أنه: (لا يجوز أن يوقف أحد أو يحبس إلاّ وفق احكام القانون) كما نصت المادة العاشرة على أنه: (للمساكن حرمة فلا يجوز دخولها إلاّ في الأحوال المبينة في القانون وبالكيفية المنصوص عليها فيه).

(1) بحر. مرجع سابق، ص 248.

أما المادة الثامنة عشرة من الدستور فقد كفلت سرية المراسلات والمخاطبات حيث جاء فيها: (تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية فلا تخضع للمراقبة أو التوقيف إلاّ في الأحوال المعينة في القانون).

وكذلك جاءت المادة الرابعة عشرة من الدستور لتحمي حرية القيام بشعائر الأديان والعقائد ما لم تكن مخلة بالنظام العام والآداب، وكذلك كفل الدستور حرية الرأي في المادة الخامسة عشرة وحرية الاجتماع وتأليف الأحزاب السياسية في المادة السادسة عشرة منه.

ومن المؤكد أن الحماية الدستورية لحق من الحقوق هي أقوى الضمانات القانونية لحماية هذا الحق.

378 ـ وبالرغم من بدء العمل بالحكومة الالكترونية في الأردن إلاّ أنه لا يوجد حتى الآن قانون لحماية الحياة الخاصة والبيانات الاسمية التي يتم تجميعها عن الأفراد من المخاطر الناجمة عن استخدام المعلوماتية وإنشاء بنوك المعلومات.

379 ـ وباستعراضنا لنصوص قانون العقوبات الأردني نجد أن المادة (355) تعالج جريمة إفشاء الأسرار الرسمية أو المهنية، حيث نصت هذه المادة على أنه: (يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من:

1- حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية وأباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقاً للمصلحة العامة.
2- كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسومات أو مخططات أو نماذج أو نسخاً منها دون أن يكون له حق الاحتفاظ بها أو دون أن تقتضي ذلك طبيعة وظيفته.
3- كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع).

380 ـ ويثار التساؤل هنا حول مدى انطباق نص هذه المادة على إفشاء البيانات الاسمية التي تعتبر إحدى صور انتهاك حرمة الحياة الخاصة في نطاق المعلوماتية.

381 ـ نشير ابتداء إلى أن السر يعرف على أنه: (واقعة أو صفة ينحصر نطاق العلم بها في عدد محدود من الأشخاص إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو أكثر في أن يظل العلم محصوراً في ذلك النطاق)[1].

والسر قد يتمثل في معلومة عن الحياة الخاصة للفرد، فمقومات الحياة الخاصة للأفراد هي مجموعة من الوقائع والصفات والأمور التي ينحصر العلم بها أما في إطار الفرد نفسه دون أحد سواه وأما يتجاوزه إلى أقرب الناس اليه دون غيرهم. وبالتالي فإن مقومات الحياة الخاصة هي أسرار بطبيعتها، ولا صعوبة في القول إن المعلومة الاسمية تتصف بالسرية[2].

382 ـ إلاّ أن الحماية المقررة بنص المادة (355) هي للمعلومات السرية الرسمية والمهنية التي تم الحصول عليها من قبل الفاعل بحكم وظيفته أو مركزه الرسمي أو بحكم مهنته. فهذا النص يضيق من دائرة التجريم فما لم يكن السر رسمياً أو مهنياً فإنه لا يكون جديراً بالحماية. وفي الواقع فإن أغلب المعلومات والبيانات المخزنة في النظام المعلوماتي التي قد تكون محلاً للإفشاء هي بيانات شخصية بعيدة عن الرسمية أو المهنية وبالتالي لا يمكن شمولها بالحماية المقررة في هذا النص.

383 ـ أما المادة (356) من قانون العقوبات الأردني فتنص على أنه:

1- يعاقب بالحبس من شهر إلى سنة كل شخص ملحق بمصلحة البرق والبريد يسيء استعمال وظيفته هذه بأن يطلع على رسالة مظروفة أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل إليه.

2- ويعاقب بالحبس مدة ستة أشهر أو بالغرامة حتى عشرين ديناراً من كان ملحقاً بمصلحة الهاتف وأفشى مخابرة هاتفية اطلع عليها بحكم وظيفته أو عمله.

أما المادة (357) فإنها تنص على أن: (كل شخص يتلف أو يفض قصداً رسالة أو برقية غير مرسلة إليه يعاقب بغرامة لا تتجاوز خمسة دنانير).

---

(1) مشار لهذا التعريف عند، الحسيني، مرجع سابق، ص65.

(2) المصدر السابق، ص 65،66.

384 ـ ويلاحظ أن النصوص السابقة لا تستوعب صور الانتهاكات لخصوصيات الأفراد التي قد تتم باستخدام التقنيات الحديثة ممثلة بجهاز الحاسوب وشبكة الانترنت، حيث من الممكن اعتراض الرسائل الالكترونية المتبادلة عبر الشبكة المعلوماتية والاطلاع على مضمونها كما يمكن التصنت على المخابرات الهاتفية التي تتم عن طريق الشبكة المعلوماتية.

385 ـ إلاّ أنه تجدر الإشارة إلى أن قانون الاتصالات الأردنية قد نص في المادة (71) على أنه: (كل من نشر أو أشاع مضمون أي اتصال بواسطة شبكة اتصالات عامة أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند قانوني يعاقب عليها بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (100) دينار ولا تزيد على (300) دينار أو بكلتا العقوبتين).

كما تنص المادة (77) على أن: (كل من أقدم على كتم رسالة عليه نقلها بواسطة شبكات الاتصال إلى شخص آخر أو رفض نقل رسائل طلب منه نقلها من قبل المرخص له أو الهيئة أو نسخ رسالة أو أفشاها أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة والرسائل المرسلة أو المستقبلة يعاقب بالحبس لمدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على ألف دينار أو كلتا العقوبتين).

386 ـ ويبدو أن المشرع الجزائي الأردني في قانون العقوبات الأردني لا بد وأن يواكب التطورات المستجدة في مجال المعلوماتية وأن يضع حماية قانونية متكاملة للحياة الخاصة للأفراد منذ بدء عملية تجميع البيانات وتخزينها ومعالجتها، حيث لا بد من وضع قواعد لهذه العملية وتقييد عملية الجمع والاستخدام لهذه البيانات بهدف محدد وغاية مشروعة ولا بد من إنشاء هيئات متخصصة لمراقبة هذه العملية حيث لا تتم إلاّ بعد أخذ موافقتها.

387 ـ بالاضافة إلى ذلك لا بد أن يتمتع الفرد صاحب البيانات أو المعلومات بمجموعة من الحقوق تتمثل في حقه بمحو المعلومات الخاطئة عنه أو إلغائها. وكذلك لا بد من حماية حق الفرد بالنسيان، فالمعلومات لا بد أن تتلف بعد مدة محددة، وكذلك حقه في تصحيح المعلومات وتعديلها إذا دعت الحاجة إلى ذلك وأخيراً لا بد أن يكون

لصاحب المعلومة الحق في الاطلاع عليها والوصول إليها وأن يكون على علم بجميع المعلومات أو البيانات المخزنة عنه[1].

388 ـ وقد أدركت العديد من الدول الأخطار المتسارعة لتكنولوجيا المعلومات على الحق في الخصوصية، الأمر الذي دفع البعض منها إلى حماية هذا الحق في الدساتير الخاصة بها كما هو الحال في الدستور الإسباني حيث نصت الفقرة الرابعة من المادة الثامنة عشرة على أن: (القانون هو الذي يحدد البيانات التي تخضع للمعالجة الالكترونية وذلك لضمان الكرامة والحصانة الشخصية والأسرية للمواطنين في ممارستهم لحقوقهم)[2].

كما نصت الفقرة الأولى من المادة الخامسة والثلاثين من الدستور البرتغالي على أن: (لكل المواطنين الحق في معرفة المعلومات التي تتعلق بهم وما تتضمنه بنوك المعلومات من بيانات خاصة بهم والاستخدامات المعدة لها ويكون لهم طلب تصحيحها أو تصويبها أو الاضافة إليها كل فترة عندما يطرأ تغيير).

وكذلك نصت الفقرة الثانية من ذات المادة على أنه: (لا يجوز استخدام الحاسبات الالكترونية في معالجة البيانات التي تتعلق بالاتجاهات السياسية أو المعتقدات الدينية أو الحياة الخاصة عدا البيانات التي تتعلق بالتعداد السكاني والبيانات غير الشخصية)[3].

389 ـ وهناك دول أخرى استحدثت قوانين خاصة لمواجهة الاعتداءات التي قد تنال الحق في الحياة الخاصة. ومن الدول الرائدة في هذا المجال فرنسا التي صدر فيها القانون رقم (17) في 6 يناير لسنة 1978 الخاص بالمعالجة الآلية للبيانات والحريات، حيث تضمن هذا القانون مجموعة من المبادئ من أهمها: أن المعالجة الآلية للمعلومات والبيانات يجب أن تكون في خدمة كل مواطن، ولا ينبغي أن يلحق هذه المعالجة ضرر بهوية الإنسان أو بحقوقه أو بحياته الخاصة ولا بحرياته الفردية أو العامة[4].

---

(1) حول الحقوق المعترف بها للفرد في مواجهة المعلوماتية انظر، منيف، مرجع سابق، ص 254،247.

(2) مشار الى هذا النص عند، قايد، مرجع سابق، ص 51.

(3) مشار الى هذا النص عند، المصدر السابق، ص 51، 52.

(4) هذا ما اشارت اليه المادة الأولى من قانون المعالجة الآلية للبيانات و الحريات لسنة 1978. مشار له عند، الحسيني، مرجع سابق، ص 56 .

وقد كفل المشرع الفرنسي لصاحب البيانات الحق في الوصول والاطلاع عليها. كما نص ذات القانون على تشكيل اللجنة القومية للمعلوماتية والحريات و الخاصة بمراقبة تنفيذ هذا القانون وقد أشار القانون إلى ضرورة الإخطار السابق للجنة قبل إجراء أي معالجة الكترونية للبيانات[1].

390 ـ أما المشرع الأمريكي فقد أصدر العديد من القوانين في هذا المجال أهمها قانون الخصوصية الذي نص على مجموعة من الضمانات لحماية البيانات الاسمية للأفراد من الانتهاك، حيث نص هذا القانون على أن الرضاء المكتوب لصاحب الشأن في المعلومات هو شرط اساسي لانتقالها داخل الادارة أو خارجها مع وجود استثناء وهو حالة تبادل المعلومات والبيانات بين الموظفين نظراً لطبيعة أعمالهم[2].

كذلك أصدر المشرع الأمريكي قانون الخصوصية والحقوق الأسرية في عام 1974 الذي أقر للأسرة الحق في مراجعة ما يتعلق بأبنائها من بيانات مسجلة لدى الجهات المختصة.

وكذلك تم إصدار قانون سياسة الاتصالات السلكية لسنة 1984، ويهدف هذا القانون إلى توفير الحماية لخصوصية الأفراد الذين يشتركون في الخدمة الهاتفية التي تجري من خلال الكابلات.

391 ـ أما في ألمانيا فقد جرم المشرع الألماني في قانون العقوبات الصادر عام 1969 إفشاء البيانات المخزنة آلياً سواء أتم بقصد أو اهمال ومنح الجهات أو الافراد حق تصحيح الأخطاء الواردة في البيانات التي تخصهم[3].

392 ــ كذلك هو الحال بالنسبة إلى كل من كندا والسويد والنرويج والدانمارك والنمسا وبلجيكيا والصين، حيث أصدرت هذه الدول قوانين لحماية الحياة الخاصة في مواجهة المعلوماتية وأخطارها.

---

(1) وقد استثنى القانون من هذا الإخطار البيانات الخاصة التي تجري معالجتها لحساب الدولة أو الهيئات العامة أو المجالس المحلية أو الأشخاص المعنوية التي تقوم بخدمة عامة التي تقررها اللوائح بعد أخذ راي اللجنة. انظر، قايد، مرجع سابق، ص 64.

(2) تم إصدار قانون الخصوصية في 1974/12/31. انظر، قايد، مرجع سابق، ص 70. وكذلك عفيفي، مرجع سابق، ص 287، 288.

(3) انظر عفيفي، مرجع سابق، ص 296.

أما بالنسبة للدول العربية فقد التزمت معظمها الصمت فيما يتعلق بحماية الحياة الخاصة للأفراد في مواجهة الأنظمة المعلوماتية وبنوك المعلومات.

393 - ومن الدول العربية القليلة التي وضعت نصوصاً لحماية البيانات والمعطيات الشخصية في مواجهة الأنظمة المعلوماتية تونس، وذلك في المواد (38 _42) من قانون التجارة الالكترونية لسنة (2000)، حيث تنص المادة 38 من ذات القانون على أنه:

(لا يمكن لمزود خدمات المصادقة الالكترونية معالجة المعطيات الشخصية، الا بعد موافقة صاحب الشهادة المعني......).

وكذلك نصت المادة 39 من ذات القانون على أنه: (باستثناء حالة موافقة صاحب الشهادة لا يمكن لمزود خدمات المصادقة الالكترونية أو أحد أعوانه جمع المعلومات الخاصة بصاحب الشهادة إلا ما كان منها ضرورياً لإبرام العقد وتحديد محتواه وتنفيذ الفاتورة وإعدادها وإصدارها).

أما المادة 42 فلقد جاء فيها أنه: (يمكن لصاحب الشهادة في كل وقت بطلب ممضي بخط اليد أو الكترونياً النفاذ إلى المعلومات الشخصية المتعلقة به وتعديلها ويشمل حق النفاذ والتعديل والدخول على جميع المعطيات الشخصية المتعلقة بصاحب الشهادة).

394 - وينص قانون الجزاء العماني كذلك على أنه: (يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين وبغرامة مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسوب في ارتكاب أحد الأفعال الآتية... انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بخصوصياتهم وتزوير البيانات أو الوثائق مبرمجة أياً كان شكلها).

المبحث الثالث
الاحتيال المعلوماتي

395 ـ إن الثورة التكنولوجية وما نجم عنها من ظهور البنوك الالكترونية والتحويل الالكتروني للاموال ضاعف من إمكانية ارتكاب الجرائم المعلوماتية وبصفة خاصة الاحتيال المعلوماتي.

فالمصارف والمؤسسات المالية في الوقت الراهن يرتكز عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لإجراء التحويلات المالية التي تتم يومياً بالطرق الالكترونية بمبالغ طائلة.

ونتيجة لظهور تقنية نقل الأموال الكترونياً عبر مصارف العالم خلال دقائق، أصبح بإمكان العملاء أصحاب الأرصدة المختلفة في البنوك القيام بهذه العملية من أي مكان في العالم ودون حاجة للذهاب إلى المصرف مباشرة.

396 ـ ويعد الاحتيال المعلوماتي من أكثر الجرائم المعلوماتية التي ترتكب على نطاق واسع في مختلف الدول و تسبب خسائر اقتصادية فادحة، الأمر الذي يشكل قلقاً متزايداً لدى المعنين بالأمر، إذ أن هذه الجريمة تهدد ثقة الأفراد بالوسائل التقنية المستحدثة لنقل الأموال.

397 ـ وتزداد خطورة الاحتيال المعلوماتي اذا علمنا أن المعلومات المتعلقة بالنواحي الاقتصادية للجهات المختلفة أصبحت مخزنة في الحواسيب والوصول إليها من أي مكان في العالم يعد أمراً سهلاً خاصة مع بروز وسائل الاتصال الحديثة، وكذلك فإن الإجراءات الأمنية التقنية التي تحاول الجهات المختلفة إحاطة هذه المعلومات بها ما زالت تعد إجراءات غير كافية حيث أن هناك ثغرات امنية كثيرة فيها يستغلها المخترقون للوصول إلى مرادهم في تحقيق الكسب غير المشروع.

فالأموال الالكترونية والودائع أصبحت هدفاً لمجرمي المعلوماتية من خلال التلاعب بمدخلات النظام المعلوماتي، بمعنى تغذية الحاسوب ببيانات غير صحيحة أو التلاعب بالبرامج أو من خلال تدخلات اخرى في معالجة البيانات.

398 ـ وللوقوف على جريمة الاحتيال المعلوماتي ألقي الضوء على ماهيته والوسائل التقنية المستخدمة في ارتكابه في (المطلب الأول)، ثم أتناول بعد ذلك مدى توافر الحماية الجزائية للمعلوماتية من خطر الاحتيال المعلوماتي في (المطلب الثاني).

المطلب الأول: ماهية الاحتيال المعلوماتي والوسائل التقنية المستخدمة في ارتكابه

399 ـ قبل أن نخوض في ماهية الاحتيال المعلوماتي والأساليب التقنية المستخدمة في ارتكابه لا بد أن نشير إلى أن عمليات الاحتيال المعلوماتي تشهد تزايداً واضحاً في منطقتنا العربية وخاصة في ظل انتشار استخدام الأنظمة المعلوماتية.

وتعد دولة الامارات المتحدة من أكثر الدول العربية تعرضاً لهذا النمط الإجرامي المستحدث نظراً لاعتمادها الكبير على أجهزة الحاسوب وعلى الشبكات المعلوماتية في إنجاز أعمالها، خاصة وأن دولة الإمارات العربية قطعت مراحل متقدمة في مجال تطبيق مشروع الحكومة الالكترونية. وقد كشف أحد المواقع الالكترونية مؤخراً أن خمسة وخمسين مواطناً إماراتياً خلال فترة وجيزة كانوا ضحية لعمليات الاحتيال المعلوماتي[1].

وفي مصر أيضاً تم القبض على عصابة من الطلبة الجامعيين قاموا بالاستيلاء على حسابات "الفيزا كارت" الخاصة بعملاء أحد البنوك عن طريق عملية احتيال الكتروني[2]. وفي اليمن تم إحباط عملية احتيال الكترونية على أحد البنوك اليمنية التي لو تمت لنجم عنها خسارة اقتصادية فادحة.

---

(1) انظر الموقع الالكتروني، www. Gn4me. com /etesalat /article. jsp

(2) انظر الموقع الالكتروني السابق. وهناك حالات احتيال معلوماتية مختلفة تم ارتكابها في دول مختلفة من العالم، مشار لها عند محمد، عادل عبد الجواد، (2000). إجرام الانترنت. مجلة الأمن والحياة. العدد (221). ص72، 73.

وبناء على ذلك سوف أتناول ابتداء تعريف الاحتيال المعلوماتي في (الفرع الاول)، ثم أعرض لأهم الوسائل التقنية المستخدمة في عملية الاحتيال المعلوماتي في (الفرع الثاني).

أولاً: تعريف الاحتيال المعلوماتي

400 ـ الاحتيال المعلوماتي ـ أو الغش المعلوماتي أو غش الحاسوب كما يطلق عليه البعض ـ تعددت التعريفات التي قيلت في شأنه.

401 ـ ومن هذه التعريفات: (إن الاحتيال المعلوماتي يتحقق كلما كانت هناك نية تحقيق ربح مادي غير مشروع للجاني، ينتج عنه خسارة مادية تلحق بالمجني عليه وكان استخدام الحاسوب وسيلة لارتكاب الاحتيال أو تسهيله أو التعجيل بتنفيذه)[1].

كما تم تعريفه أنه: (كل سلوك احتيالي يرتبط بعملية التحسيب الالكتروني بهدف كسب فائدة أو مصلحة مالية)[2].

402 ـ أما هيئة الأمم المتحدة فلقد عرفت الاحتيال المعلوماتي أنه: (إدخال البيانات أو محوها أو تعديلها أو كبتها أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص آخر، بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر)[3].

كما عرفته إحدى الدراسات المسيحية التي أجريت في الولايات المتحدة أنه: (فعل أو مجموعة من الأفعال غير المشروعة والمتعمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذي قيمة، ويكون نظام الحاسوب لازماً لارتكابها)[4].

---

(1) قورة، مرجع سابق، ص 443.

(2) صالح، واقع جرائم الحاسوب ... مرجع سابق، ص 7. وعرفه البعض كذلك إنه: (كل تصرف احتيالي يتعلق بالمعلوماتية التي من خلالها ينوي احدهم تحقيق كسب غير مشروع) انظر، رياح، غسان، قانون حماية الملكية الفكرية والفنية الجديد مع دراسة مقارنة حول جرائم المعلوماتية، بدون ناشر، ص103.

(3) مشار له عند، قندح، خليل، الجرائم المرتكبة بواسطة المعلوماتية، ورقة عمل مقدمة لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، اربد، في الفترة ما بين 12 ـ 14 تموز، 2004، ص 6.

(4) عرب، دليل أمن المعلومات والخصوصية... مرجع سابق، ص 416.

403 ـ ويذهب البعض الآخر[1] إلى تعريفه أنه: (التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادياً، يختزنها النظام المعلوماتي أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة أو أية وسيلة أخرى من شأنها التأثير على الحاسوب حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير).

وهذا التعريف حاول الإحاطة بالجوانب المختلفة لجريمة الاحتيال المعلوماتي، وهو التعريف الذي نذهب معه.

404 ـ والربح غير المشروع الذي يحققه الجاني باعتباره نتيجة لارتكاب جريمة الاحتيال المعلوماتي قد يتخذ أحد شكلين:

الأول: يتحقق بشكل مباشر، كما لو قام الفاعل بتحويل مبلغ من المال إلى حسابه.

الثاني: يتحقق بشكل غير مباشر عندما يتخلص الفاعل من تسديد مبلغ من المال يقع على عاتقه التزاماً بأدائه، ومن الأمثلة على ذلك الاستخدام غير المصرح به من قبل الفاعل للشيفرة الخاصة لشخص آخر للدخول إلى إحدى النظم المعلوماتية، ويترتب على ذلك أن يتحمل المجني عليه نفقات هذا الدخول.

405 ـ وتجدر الإشارة إلى أن الاحتيال المعلوماتي شأنه في ذلك شأن جرائم المعلوماتية بوجه عام، يمكن ان يكون مرتكبه من المصرح لهم باستخدام الحاسوب والدخول إلى نظامه أو أن يكون غير مصرح لهم بذلك.

إلاّ أنه من الثابت من واقع التجربة العملية أن حالات الاحتيال بواسطة الحاسوب لجني المال تأتي في جانبها الأكبر من داخل الجهات المجني عليها لا من خارجها، فمرتكبي الاحتيال المعلوماتي هم عادة أشخاص لديهم السلطة في التعامل مع المعلومات التي يحتويها النظام المعلوماتي، حتى أنه قد أطلق على التحايل المعلوماتي أنه جريمة داخلية إشارة إلى حدوثه داخل المؤسسة المجني عليها وبواسطة أحد المنتمين إليها.

(1) قورة، مرجع سابق، ص 444.

وقد أثبتت دراسة أجريت في ألمانيا أن أكثر من 90% من حالات التلاعب المعلوماتي التي تم اكتشافها قد تم ارتكابها بواسطة عاملين في المؤسسات المجني عليها[1].

وفي دراسة أجراها معهد نيويورك للأبحاث تبين أن ثلاثة ارباع حالات الاحتيال المرتبط بالحاسوب قد تمت عن طريق أشخاص من داخل المؤسسات المجني عليها.

وفي دراسة اخرى أجريت في السويد على مجموعة من قضايا الاحتيال التي استخدم الحاسوب في ارتكابها ومجموعة أخرى تضم (180) قضية احتيال لا علاقة لارتكابها بالأنظمة المعلوماتية، تبين أن 81% من مرتكبي الاحتيال المرتبط بالحاسبات الآلية ينتمون وظيفياً إلى الجهات المجني عليها[2].

ثانياً: وسائل الاحتيال المعلوماتي

406 ـ أساليب ارتكاب جريمة الاحتيال المعلوماتي متنوعة ومتطورة تبعا للتطور التكنولوجي الذي تشهده المعلوماتية، وكان لشيوع انظمة التحويل الالكتروني للاموال دور كبير في تنامي هذه الجريمة وتطور اساليب ارتكابها وخاصة مع زيادة عدد المبرمجين والمشتغلين في مجال الانظمة المعلوماتية.

407 ـ وسنقوم بعرض أهم الأساليب التقنية المستخدمة في ارتكاب جريمة الاحتيال المعلوماتي ونعرض كذلك لبعض الامثلة العملية التي تم استخدام هذه الأساليب التقنية فيها لفهم طبيعة عملها بشكل أوضح.

1- التلاعب في مرحلتي إدخال وإخراج البيانات:

408 ـ التلاعب بالبيانات المدخلة إلى جهاز الحاسوب يعد من أكثر حالات الاحتيال المعلوماتي حدوثاً نظراً لما يتميز به من سهولة. وقد ظهر ان 62% من حالات الاحتيال المعلوماتي التي تم اكتشافها في الولايات المتحدة الأمريكية حتى عام 1984 تنطوي على تلاعب بالبيانات قبل أو أثناء إدخالها إلى جهاز الحاسوب[3].

(1) فورة، مرجع سابق، ص 445.

(2) المصدر السابق، ص 446.

(3) انظر الموقع الالكتروني، www.alyaseer.gov.sa/forum/topic.asp.archive.

وتتمثل عملية إدخال المعلومات المزورة في تغذية النظام المعلوماتي بالمعلومات والبيانات المراد معالجتها آليا، وقد تتم عملية الإدخال عن طريق الشخص نفسه الذي قام بالتلاعب في المعلومات، أو عن طريق شخص آخر قد يكون حسن النية.

409 ـ وتتنوع وسائل التلاعب بالمعلومات و البيانات في هذه المرحلة سواء أتمّ ذلك اثناء عملية الإدخال أو في مرحلة إعداد المعلومة للإدخال، ويمكن حصرها في ثلاثة وسائل رئيسة[1]:

الوسيلة الأولى:

تتمثل هذه الوسيلة في تغيير المعلومات والبيانات المراد ادخالها إلى النظام دون أن يتضمن ذلك حذفاً لجزء أو أجزاء منها، سواء أتمّ ذلك في مرحلة الادخال أو قبل ذلك أي أثناء إعداد هذه المعلومات للإدخال. وقد يكون هذا التغيير كلياً، أي يشمل المعلومة بأكملها أو جزئياً يتعلق بجزء دون الآخر. كما قد يتمثل في إضافة جزء لها ليس فيها او استبدال معلومة بأخرى، ويؤدي كل ما سبق إلى تغيير معنى المعلومة حيث تصبح غير معبرة عن الحقيقة التي كانت تمثلها.

الوسيلة الثانية:

من وسائل التلاعب بالبيانات في مرحلة الإدخال قد تنطوي على حذف لجزء من المعلومة أو لعدة أجزاء منها، بل إن الأمر قد يتعدى ذلك إلى حذف المعلومة بأكملها أو عدم إدخالها إلى النظام المعلوماتي، ويترتب على ذلك أيضاً تغيير معنى المعلومة أو عدم وجودها ابتداء.

الوسيلة الثالثة:

تتمثل هذه الوسيلة في إعاقة المعلومة عن أداء وظيفتها ويتم ذلك عن طريق إدخال المعلومة مع إخفائها وذلك بأن يتم إدخالها في غير المكان المخصص لها، وهو ما يؤدي إلى إعاقة هذه المعلومة عن أداء الدور الذي كان مقرراً لها.

---

(1) انظر، قورة، مرجع سابق، 453، 454.

410 ـ ومن الأمثلة على الاحتيال المعلوماتي الذي يتم عن طريق التلاعب بالبيانات المدخلة:

1- قيام أحد مدخلي البيانات العاملين في إحدى الشركات المساهمة عام 1994 في الأردن بتسجيل (87300) سهم بأسماء شركاء وهميين وإخراج شهادات بملكية الأسهم لمالكيها، ومن ثم قيامه ببيعها في السوق المالية وبمبلغ يزيد على مائة وتسعين ألف دينار أردني[1].

2- قام موظف يعمل في مجال معالجة البيانات في أحد البنوك السويسرية الكبرى بالتلاعب في المعاملات المالية الخارجية للمصرف ونتيجة لذلك تمكن من الاستيلاء مع بعض شركائه على مبالغ طائلة. حيث كان يمنح هذا الموظف بحكم عمله كمشغل بيانات ومراجعها وصول بعض أوامر تحويل النقود إلى قسم الترميز ليقوم هو بعملية إدخالها إلى الحاسوب، غير أنه بدلاً من إدخال القيمة الفعلية لكل امر تحويل، كان يدخل هذه القيمة مضروبة في ألف، وقد تمكن بهذه الطريقة من الاستيلاء على (700000) فرنك سويسري من أموال البنك[2].

411 ـ أما التلاعب في مرحلة إخراج البيانات فهذه الوسيلة تعد أقل حدوثاً بالمقارنة بغيرها من وسائل الاحتيال المعلوماتي، ففي التقرير الصادر عن لجنة المراجعة في المملكة المتحدة عام 1985 كانت هناك حالتان فقط من بين (77) حالة احتيال معلوماتي قد تمت عن طريق التلاعب بالبيانات في مرحلة إخراج المعلومات. فالتلاعب وفقاً لهذه الوسيلة ينصب على البيانات في اللحظة التي يتم فيها إخراجها من جهاز الحاسوب، فالفرض في هذه الحالة أن المعلومات دخلت صحيحة إلى النظام المعلوماتي وأن التلاعب تم قبل عملية إخراج المعلومات[3].

(1) قندح، مرجع سابق، ص 8.

(2) محمود، مرجع سابق، ص 104.

(3) انظر، قورة، مرجع سابق، ص 458، 459.

2- التلاعب في البرامج:

412 ـ تتميز هذه الوسيلة أنها على قدر كبير من التعقيد، وتحتاج الى خبرة ومعرفة فنية في مجال البرمجة، كما أنها تعتبر من أكثر وسائل الاحتيال المعلوماتي خطورة. ويتم التلاعب في البرامج بصفة عامة عن طريق إحدى وسيلتين:[1]

الوسيلة الأولى:

تتمثل هذه الوسيلة في تغيير البرامج المطبقة بالفعل داخل المؤسسة المجني عليها، بإدخال تعديلات غير مرخص بها على البرامج المستخدمة. فكثير من البرامج بعد إعدادها واختبارها قد تمر ببعض التعديلات لتصويب أخطاء اكتشفت بعد العمل بها وهو ما يتيح في هذه الحالة إدخال تغييرات من شأنها أن تساعد الجاني على إتمام جريمته وكذلك إخفائها. كما قد يتم إجراء هذا التعديل عن طريق استخدام البرامج الخبيثة (الفيروسات).

الوسيلة الثانية:

تتمثل هذه الوسيلة في تطبيق برامج إضافية، وهذه البرامج الإضافية قد يتم كتابتها عن طريق الجناة أنفسهم أو قد تكون برامج معدة سلفاً تهدف بشكل أساسي إلى تعديل المعلومات في الحواسيب عن طريق إجراء تعديلات مباشرة في ذاكرتها.

413 ـ ومن الأمثلة التي تبين ماهية التلاعب بالبرامج كوسيلة من وسائل الاحتيال المعلوماتي:

1- قيام مبرمج يعمل بأحد البنوك في الولايات المتحدة الامريكية بتعديل برنامج إدارة الحسابات الخاصة بالبنك، حيث يضيف عشرة سنتات لمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات ودولاراً واحداً على الحسابات التي تتجاوز عشرة دولارات، وذلك باستخدام تقنية تدعى

(1) انظر، المصدر السابق، ص 462، 463.

تقنية (Salami)[1]. وقد تم تسجيل المصاريف الزائدة في حساب خاص فتحه بإسم مستعار هو (Zzwicke) وبهذه الطريقة حصل على عدة مئات من الدولارات كل شهر. وكان بالإمكان أن يستمر هذا الأمر الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له وفقاً للترتيب الابجدي للحروف وحينئذ اكتشف عدم وجود ما يسمى (Zzwicke)[2].

2- تقنية أخرى تدعى (Perru que)، تقوم على برمجة الحاسوب حيث يستقطع بعض السنتيمات (Cenitmes) من الإيداعات الدورية وتحويلها إلى حسابات خاصة. وبهذه التقنية استطاع مستخدم بإحدى شركات التأمين برمجة الحاسوب حيث يستقطع السنتيمات من كل عمليات الشركة وتم تحويلها إلى حسابه السري[3].

414 ـ كما إن التلاعب بالبرامج قد يتم عن طريق خلق برنامج وهمي يصمم خصيصاً بهدف ارتكاب الجريمة. ومن الأمثلة على ذلك ما قامت به شركة أمريكية من اصطناع وثائق تأمين لاشخاص وهميين بلغ عددها (64000) وثيقة وبعد ذلك قامت الشركة ببيع هذه الوثائق لأشخاص آخرين وحصلت في مقابل ذلك على عمولات من شركات التأمين التي تعمل لحسابها وقد حصل الجناة من هذه العملية على مبلغ (200) مليون دولار[4].

(1) يطلق الخبراء اسم (Salami) على عملية استقطاع الشرائح الصغيرة من حسابات متعددة لصالح فرد واحد، ويطبق هذا الأسلوب بكثرة في البنوك حيث تقرر الفوائد على الحسابات الجارية التي ترتضي حساباتها الشهرية بازالة الكسور العشرية التي تمثل مبالغ لاتكاد تذكر، حينئذ يكون من السهل على مبرمج البنك ان يصمم حساب الفوائد دون أخذ الكسور العشرية في الاعتبار والفرق بين الحساب الصحيح والحساب دون الكسور العشرية يذهب لحسابه الخاص، وفي كل عملية يكون الفارق غير واضح لجميع العملاء ولكنه مجزي للغاية على المدى الطويل. انظر، الصغير، مرجع سابق، ص47.

(2) مشار لهذه الواقعة عند، الشوا، مرجع سابق،ص 78. وكذلك، محمود، مرجع سابق، ص121.

(3) الشوا، مرجع، سابق، ص 79.

(4) مشار لهذه الواقعة عند، الصغير، مرجع سابق، ص 49،50.

3- التلاعب في البيانات التي يتم تحويلها عن بعد:

415 ـ هذه الوسيلة من وسائل الاحتيال المعلوماتي يتم ارتكابها عادة من قبل أشخاص من خارج المؤسسة المجني عليها. وقد كان للتزايد الكبير في استخدام نظم معالجة البيانات عن بعد في السنوات الاخيرة تأثير كبير في تطوير الوسائل المختلفة المستخدمة في مجال تكنولوجيا المعلومات.

416 ـ فالتلاعب في البيانات عن طريق النهاية الطرفية أياً كان موقعها جعل الاحتيال أكثر سهولة من ناحية وأكثر صعوبة في اكتشافه من ناحية أخرى، فيكفي أن يكون الحاسوب متصلاً بوحدة التشغيل المركزية عن طريق شبكة الخطوط الهاتفية العادية أو غيرها من وسائل الاتصال حتى يتمكن الفاعل من إتمام عملية الاحتيال من داخل منزله مستخدماً لوحدته الطرفية دون الحاجة إلى الدخول إلى المؤسسة المجني عليها[1].

ووفقاً لهذه الوسيلة التقنية يمكن للجاني أن يقترف السلوك الإجرامي المكون للركن المادي لجريمته في دولة ما، وتتحقق النتيجة الإجرامية في دولة أخرى.

417 ـ ومن الحالات التي تم فيها استخدام هذه الطريقة لاقتراف جريمة الاحتيال المعلوماتي، قيام خبير برمجة يعمل في مصرف أمريكي ويدعى (Stanly Kifkin) بالوصول إلى غرفة توصيلات النقل لبنك (Security Pacific) وتمكن من الحصول على الشيفرة التي يستخدمها هذا البنك. وقام بعد ذلك بالاتصال بشبكة معلومات البنك عن طريق الهاتف مستخدماً الشيفرة التي حصل عليها وقام بزرع فيروس في الشبكة مهمته تحويل مبالغ مالية من حسابات العملاء إلى حسابه الخاص في نيويورك[2].

4- استعمال شيفرة غير صحيحة للدخول إلى نظام مدفوع الأجر:

تعد هذه الوسيلة صورة من صور الاحتيال المعلوماتي التي قد يستعين بها الجاني لتحقيق كسب غير مشروع.

---

(1) قورة، مرجع سابق، ص 466، 467.

(2) مشار لهذه الواقعة لدى، فوريستر، مرجع سابق، ص 402.

418 ـ ويعد استعمال شيفرة غير صحيحة من أهم الوسائل للدخول غير المشروع إلى نظام مدفوع الأجر. والمقصود باستعمال شيفرة غير صحيحة هو الدخول إلى الأنظمة المعلوماتية مدفوعة الأجر باستعمال شيفرة مملوكة إلى شخص آخر أو باستعمال شيفرة مملوكة للنظام نفسه. فليس المقصود أن تكون هذه الشيفرة غير صحيحة في ذاتها وإنما تستمد عدم صحتها من استخدامها من قبل شخص لاحق له في ذلك[1].

المطلب الثاني: الحماية الجنائية للمعلوماتية من خطر الاحتيال المعلوماتي في قانون العقوبات الأردني

419 ـ الاحتيال المعلوماتي هذه الجريمة التي يزداد معدل ارتكابها يوماً بعد يوم وتشكل في ذات الوقت خطراً داهماً على المؤسسات المالية وبالتالي على الاقتصاد الوطني، لا بد من مواجهتها تشريعياً وهذا الأمر أدركته كثير من الدول فأفردت لها نصوصاً خاصة تراعي طبيعتها والأساليب المستخدمة في ارتكابها.

والسؤال الذي يثار في هذا الصدد هو حول مدى إمكانية انطباق النصوص الخاصة بجريمة الاحتيال في قانون العقوبات الأردني على جريمة الاحتيال المعلوماتي. وللإجابة عن هذا التساؤل استعرض في (الفرع الأول) الأركان العامة لجريمة الاحتيال في قانون العقوبات الأردني، ثم سأقوم بالبحث في مدى انطباق هذه الاركان على جريمة الاحتيال المعلوماتي في (الفرع الثاني).

أولاً: الأركان العامة لجريمة الاحتيال في قانون العقوبات الأردني

420 ـ تناول المشرع الأردني جريمة الاحتيال في الفصل الثاني من الباب الحادي عشر في قانون العقوبات الأردني تحت عنوان (في الاحتيال وسائر ضروب الغش)، وذلك في المواد (417 ـ 421).

421 ـ وقد نصت المادة (417) من قانون العقوبات الأردني أن: (كل من حمل

---

(1) قورة، مرجع سابق، ص 469.

الغير على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء فاستولى عليها احتيالاً:

أ- باستعمال طرق احتيالية من شأنها إيهام المجني عليه بوجود مشروع كاذب أو حادث أو أمر لا حقيقة له أو إحداث الأمل عند المجني عليه بحصول ربح وهمي أو بتسديد المبلغ الذي أخذ بطريق الاحتيال أو الايهام بوجود سند دين غير صحيح أو سند مخالصة مزور، أو

ب- بالتصرف في مال منقول أو غير منقول وهو يعلم أنه ليس له صفة للتصرف به، أو

ت- باتخاذ اسم كاذب أو صفة غير صحيحة.

عوقب بالحبس من ثلاثة اشهر إلى ثلاث سنوات وبالغرامة من مائة دينار إلى مائتي دينار).

422 ـ وكما هو واضح من نص المادة (417) لم يعرف المشرع الجزائي الأردني ومثل غيره من المشرعين في الدول الأخرى جريمة الاحتيال[1].

423 ـ أما في الفقه، فقد عرف البعض جريمة الاحتيال أنها:[2] (كل تظاهر أو إيحاء يكون صالحاً لايقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة النصب هو من جازت عليه حيله الجاني فانخدع بها وسلمه ماله).

424 ـ وقد عرفت محكمة التمييز الأردنية فعل الاحتيال كذلك أنه: (فعل الخداع من المحتال ليحمل المجني عليه على تسليمه ماله لكي يستولي عليه، وهو ما كان ليقبل بهذا التصرف لو عرف الحقيقة)[3].

---

(1) لم يعرف المشرع المصري جريمة الاحتيال (أو النصب وهي التسمية الواردة في قانون العقوبات المصري) وذلك في المادة 336 من قانون العقوبات المصري. وكذلك الحال بالنسبة للمشرع اللبناني في المادة (655) من قانون العقوبات اللبناني، وايضا هذا هو الحال عند المشرع الفرنسي والذي لم يعرف جريمة الاحتيال عند نصه عليها في المادة 405 من قانون العقوبات الفرنسي.

(2) الشوا، ثورة المعلومات ... مرجع سابق، ص 123.

(3) تمييز جزاء رقم 85/134، مجلة نقابة المحامين الأردنيين، العددين التاسع والعاشر، السنة الرابعة والثلاثين، ص1388.

425 ـ وتعد جريمة الاحتيال من جرائم الأموال التي يهدف المشرع بتجريمه إياها إلى حماية حق الملكية. حيث يتمثل هذا الاعتداء في نية سلب ثروة الغير كلها أو بعضها، أي نية تملك المال، وهي تعني إرادة مباشرة السلطات التي تنطوي عليها حق الملكية.

وبالاضافة إلى حماية حق الملكية، يحمي المشرع بتجريمه الاحتيال مصلحة أخرى وهي حرية الارادة وسلامتها. وتتمثل حمايته لسلامة الإرادة في تجريمه أسلوب الاحتيال الذي يلجأ إليه الجاني، فيوقع المجني عليه في الغلط فيسلمه محل الجريمة تحت سطوة هذا الغلط، فإرادة المجني عليه حين سلم المال كانت إرادة غير سليمة[1].

426 ـ ويتبين لنا من خلال استعراض نص المادة (417) من قانون العقوبات الأردني أنه لا بد من توافر ثلاثة أركان لقيام جريمة الاحتيال وهي:

- محل الجريمة.
- الركن المادي.
- الركن المعنوي.

427 ـ فيما يتعلق **بالركن الأول** وهو محل جريمة الاحتيال، لا بد أن يكون مالاً ذا طبيعة مادية. ولا يمكن أن يكون محل جريمة الاحتيال الإنسان أو المنفعة حتى ولو كان بالامكان تقييم الأخيرة مادياً.

أما بالنسبة لطبيعة المال محل جريمة الاحتيال فيمكن أن يكون مالاً منقولاً أو غير منقول[2]، أو أسناداً تتضمن تعهداً او إبراء أو أوراقاً تجارية، وذلك بخلاف بعض التشريعات الأخرى التي أخرجت من دائرة الاحتيال الأموال غير المنقولة كالعقارات

(1) قورة، مرجع سابق، ص 438، 439.

(2) تجدر الاشارة إلى ان (العقار ـ وهو من الأموال غير المنقولة ـ لا يكون محلاً لجريمة الاحتيال إلاّ بطريقة غير مباشرة وذلك من خلال الاستيلاء بإحدى وسائل الاحتيال على عقد بيعة أو رهنه أو على سند رتب للجاني حق ارتفاق عليه، فعملية الاستيلاء الفعلي على عقار وحيازته تامة غير ممكنة من قبل أي شخص) . انظر، نجم وصالح، مرجع سابق، ص 440، 441.

كما هو الحال في قانون العقوبات المصري[1]. ولا بد أن يكون هذا المال مملوكاً للغير وليس للجاني الحق أو السلطة للتصرف فيه.

428 - أما **الركن المادي** لجريمة الاحتيال فيقوم على ثلاثة عناصر أساسية هي:

العنصر الأول: نشاط إيجابي يقوم به الجاني ويتمثل هذا النشاط في استخدام الفاعل لوسيلة من الوسائل الاحتيالية التي حددها المشرع في المادة (417) من قانون العقوبات على سبيل الحصر، وهذه الوسائل تتمثل في :

1- إستعمال طرق احتيالية من شانها إيهام المجني عليه بوجود مشروع كاذب أو حادث أو أمر لا حقيقة له أو إحداث الأمل عند المجني عليه بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الاحتيال أو الإيهام بوجود سند دين غير صحيح أو سند مخالصة مزور.

ولم يقم المشرع الجزائي الأردني بوضع تعريف قانوني للطرق الاحتيالية؛ وعلة ذلك أن هذه الطرق من الصعب حصرها وشمولها في تعريف جامع مانع، إذ أنها تتطور وتنمو وتواكب المستجدات العلمية والتقنية.

وقد سعى الفقه إلى وضع تعريف لهذه الطرق الاحتيالية، فتم تعريفها أنها: (كل كذب مصحوب بوقائع خارجية أو أفعال مادية يكون من شأنها توليد الاعتقاد لدى المجني عليه بصدق هذا الكذب الامر الذي يدفعه إلى تسليم ما يراد منه تسليمه طواعية واختياراً)[2].

وبناءً على ما تقدم، فلا بد أن يكون هناك كذب قد صدر عن الجاني وأن يكون من شأن هذا الكذب تغيير الحقيقة، ولا بد من أن يرافق هذا الكذب مظهر خارجي يؤكد الكذب ويدعمه وتتمثل هذه المظاهر الخارجية بالإستعانة بالغير أو بالإستعانة بأوراق غير صحيحة أو القيام بأعمال مادية أو استغلال الصفة أو الثقة.

(1) المصدر السابق، ص 440.

(2) انظر، نجم وصالح، مرجع سابق، ص 447.

2- الوسيلة الثانية من الوسائل الاحتيالية هي تصرف الفاعل في مال منقول أو غير منقول هو يعلم أنه ليس له صفة للتصرف به.

3- أما الوسيلة الثالثة فهي اتخاذ الفاعل اسماً كاذباً أو صفة غير صحيحة.

العنصر الثاني: حصول النتيجة الإجرامية هي العنصر الثاني للركن المادي في جريمة الاحتيال وتتمثل هذه النتيجة في تسليم المال من المجني عليه إلى الجاني، فحتى تقوم جريمة الاحتيال لا بد أن تؤدي الوسائل الاحتيالية التي نص عليها المشرع إلى إيقاع المجني عليه في غلط يحمله على تسليم ماله إلى الجاني طواعية.

ولا بد أن تكون إرادة المجني عليه لحظة التسليم معيبة، أي أنه سلم المال نتيجة الغلط الذي وقع فيه. ولا بد كذلك من أن يكون الشخص الذي قام بالتسليم أو أمر به هو ذات الشخص الذي وقع نتيجة الاحتيال في الغلط، كما يجب أن يكون هدف الجاني لحظة استلام المال هو الاستيلاء عليه، وأخيراً يجب أن يكون التسليم لاحقاً لاستخدام الأسلوب الاحتيالي لا سابقاً عليه[1].

العنصر الثالث: وجود علاقة سببية تربط بين النشاط الإيجابي الذي قام به الفاعل والنتيجة الإجرامية. حيث أن النتيجة الاجرامية المتمثلة بتسليم المجني عليه المال للجاني لا بد أن تكون محصلة للاسلوب الاحتيالي الذي استخدمه الفاعل وأدى إلى وقوع المجني عليه في الغلط مما حدا به إلى تسليم المال، أما إذا تم التسليم بناء على سبب آخر انقطعت علاقة السببية.

429 ـ أما **الركن الثالث** والأخير في جريمة الاحتيال فهو الركن المعنوي المتمثل في القصد الجرمي العام والقائم على عنصري العلم والارادة: علم الجاني بكلّ عناصر جريمة الاحتيال كما حددها المشرع، وفي الوقت ذاته اتجاه إرادته إلى اقتراف النشاط الإيجابي وهو استخدام إحدى الوسائل الاحتيالية التي وردت في المادة 417 على سبيل الحصر واتجاه إرادة الجاني ايضا إلى تحقيق النتيجة الجرمية.

وإلى جانب القصد العام لا بد ان يتوافر لدى الجاني القصد الخاص والمتمثل في نية تملك مال الغير.

(1) نجم و صالح، مرجع سابق، ص 474، 475.

ثانياً: مدى إمكانية انطباق نصوص جريمة الاحتيال التقليدية على جريمة التحايل المعلوماتي

430 ـ تثير مسألة مدى إمكانية انطباق نصوص جريمة الاحتيال التقليدية على التحايل المعلوماتي الجدل حول العديد من المسائل والنقاط التي تستدعي البحث والدراسة. فالتحايل المعلوماتي جريمة على درجة من التعقيد سواء أكان ذلك من حيث طبيعة المحل الذي ترد عليه أو من حيث الوسائل التي ترتكب من خلالها.

431 ـ ولا بد ابتداء من دراسة مدى إمكانية ممارسة الأفعال الاحتيالية على الحاسوب والنظام المعلوماتي المرتبط به، بمعنى آخر مدى صلاحية الحاسوب لأن يكون مجنياً عليه. وكذلك لا بد أن نسلط الضوء على مدى اعتبار تسليم الأموال الكتابية أو البنكية عن طريق عملية القيد الكتابي تسليماً مادياً تتحقق من خلاله النتيجة الاجرامية لجريمة الاحتيال، وأخيراً لا بد من تناول مدى امكانية اعتبار الوسائل الاحتيالية التي يلجأ إليها الجاني لارتكاب الاحتيال المعلوماتي من قبيل الطرق الاحتيالية التي نص عليها المشرع الجزائي الأردني في المادة (417) من قانون العقوبات الاردني.

1- مدى امكانية الاحتيال على الحاسوب والنظام المعلوماتي المرتبط به:

432 ـ إذا كان الاحتيال في صورته التقليدية ينطوي على اتصال بين الجاني وبين شخص آخر يمارس الجاني حياله نشاطه الإجرامي، فإن الاحتيال المعلوماتي يقوم على اتصال بين الفاعل ونظام الحاسوب فقط، ويبدو ذلك واضحاً في حالة التحويل الالكتروني غير المشروع للأموال الكترونياً دون تدخل لأي عنصر بشري.

433 ـ وقد أثارت مسألة الاحتيال على الحاسوب بوصفه مجرد آلة جدلاً فقهياً، وكانت الآراء منقسمة في اتجاهين:

الاتجاه الأول: يذهب إلى ان الحاسوب هو مجرد وسيط للتحايل وأن الطبيعة المعلوماتية لجرائم الحاسوب لا تضيف جديداً في مجال الاحتيال التقليدي إلا مجرد الوسيلة المستخدمة[1].

---

(1) قشقوش، جرائم الحاسب الإلكتروني ... مرجع سابق، ص 152.

فالاحتيال على الحاسوب لسلب مال الغير، تتحقق به الطرق الاحتيالية باعتبار أن ما يتم هو أكاذيب تدعمها وقائع خارجية تتمثل في المعلومات والبيانات التي يتم إدخالها إلى الحاسوب، وذلك على اعتبار أن هناك دائماً شخصاً طبيعياً يقف وراء النظام المعلوماتي، الأمر الذي يمكن القول معه إنه هو الذي خدع بالطرق الاحتيالية التي لجأ اليها الجاني.

ويشير جانب من الفقه الفرنسي المؤيد لهذا الاتجاه إلى أن المشرع انحصر تفكيره عند صياغة القانون في العلاقات القائمة بين البشر، ولم يعتقد يوماً أن هذه العلاقات ستتطور لتصبح بين الآلة والإنسان، وهذه المسألة ليست بذات قيمة وفقاً لهذا الرأي فالانسان هو الذي يقف وراء آلته[1].

كما يدعم هذا الجانب من الفقه وجهة نظره بما قضت به محكمة النقض الفرنسية بتطبيق عقوبة جريمة الاحتيال على شخص دخل بسيارته إلى أماكن انتظار السيارات، وبدلا من وضع النقود الأصلية المطلوبة في عداد أماكن الانتظار قام بوضع قطعة معدنية عديمة القيمة فيه وترتب على ذلك تشغيل الماكينة وتحريك العقارب. حيث أسست المحكمة حكمها على أن وضع قطعة معدنية عديمة القيمة في العداد يعد من قبيل الطرق الاحتيالية[2].

ووفقاً لهذا الاتجاه فإنه يمكن تطبيق النصوص التقليدية في قانون العقوبات على جريمة التحايل المعلوماتي.

الاتجاه الثاني: يرى هذا الاتجاه أنه لا يمكن القول بصلاحية نظام الحاسوب لوقوع فعل الاحتيال عليه وبالتالي لا يمكن اعتباره مجنياً عليه، إذ أنه مجرد آلة. كما أن النصوص القانونية التقليدية التي وضعت لمواجهة جريمة الاحتيال تفترض بأن الطرق

---

(1) الشوا، ثورة المعلومات ... مرجع سابق، ص 124. كذلك انظر، قورة، مرجع سابق، ص 575.

(2) انظر، الشوا، ثورة المعلومات ... مرجع سابق، ص 124، 125.

وتجدر الإشارة إلى أن هناك من يرى (أنه وبتحليل هذا الحكم القضائي الفرنسي نجد ان هناك خداعاً مباشراً حدث للإنسان وفقاً لما هو وارد في نص المادة 405 من قانون العقوبات الفرنسي وهي المادة المتعلقة بجريمة الاحتيال، وذلك على أساس أن وضع قطعة معدنية يترتب عليه تشغيل الماكينة وتحريك عقارب العداد، مما أوهم المراقب المالي بأن الجاني قد دفع أجرة الانتظار في الموقف). انظر، عفيفي، مرجع سابق، ص161.

الاحتيالية لا بد أن تقع بين شخصين طبيعيين، فالادعاء الكاذب يفترض علاقة مباشرة بينهما. مما يسوغ القول بأن الطرق الاحتيالية نطاقها العلاقات الانسانية وليس مجرد اجهزة آلية صماء[1].

ووفقاً لهذا الاتجاه فلا بد من استحداث نصوص عقابية تجرم الاحتيال المعلوماتي وذلك بما يتناسب مع طبيعة هذه الجزيمة المستحدثة، وهو الاتجاه الذي نذهب معه إذ أن محاولة مد نصوص القانون لتشمل جريمة الاحتيال المعلوماتي يصطدم مع مبدأ شرعية الجريمة والعقوبة.

434 ـ أما بالنسبة إلى موقف التشريعات المختلفة من إمكانية ممارسة الاحتيال على نظام الحاسوب وبالتالي إيقاعه في الغلط كان هناك ثلاثة اتجاهات:

الاتجاه الأول: وفقاً لهذا الاتجاه التشريعي لا يمكن خداع نظام الحاسوب بوصفه مجرد آلة، حيث لا بد أن يكون الفاعل قد خدع انساناً مثله. وبالتالي لا يمكن تطبيق النص القانوني الخاص بجريمة الاحتيال التقليدية على جريمة التحايل المعلوماتي.

وهذا ما يذهب إليه المشرع الأردني في المادة (417) من قانون العقوبات الأردني حيث استعمل المشرع لفظ (الغير)، بقوله في مطلع المادة (كل من حمل الغير على تسليمه...) فالمشرع يفترض ان المجني عليه انسان يتمتع بالشعور والارادة وقادر على التفكير وليس مجرد آلة.

ـ وهذا ما ذهب إليه أيضاً كل من المشرع المصري واللبناني والألماني والدانماركي والايطالي[2].

الاتجاه الثاني: تمثله تشريعات الدول الانجوسكسونية ويرجع السبب في إمكانية تصور وقوع الاحتيال على الحاسوب وإيقاعه في الغلط وفقاً لهذه التشريعات ليس بسبب وجود نص صريح يقر بذلك، وإنما بسبب النصوص الواردة فيها والمتعلقة

(1) المصدر السابق، ص160.

(2) عفيفي، مرجع سابق، ص151.

بجريمة الاحتيال التي تتسم بالعموم والشمول، حيث يمكن الاستناد إلى هذه السمة أحيانا لتطبيق أحكام تلك النصوص على فعل الاحتيال الواقع على الحاسوب[1].

الاتجاه الثالث: يمثله التشريع الأمريكي، حيث اتجهت بعض الولايات الأمريكية إلى تعديل النص الخاص بالاحتيال في قانون العقوبات ليشمل الاحتيال على الآلة، كما هو الحال بولاية آلاسكا.

2- مدى اعتبار تسليم الأموال الكتابية (البنكية) عن طريق عملية القيد الكتابي تسليماً مادياً تتحقق من خلاله النتيجة الجرمية لجريمة الاحتيال:

435 ـ المقصود بالنقود الالكترونية (البنكية أو الكتابية)، تلك النقود التي يتم تداولها عن طريق نظم المعالجة الآلية للمعلومات، وبصفة خاصة في ظل نظم التحويل الالكترونية للأموال التي تعتمد على نظام (Online) بصورة متكاملة حيث يتم نقل الأموال من خلاله بشكل فوري[2].

وتقتضي جريمة الاحتيال التقليدية أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية وهي تستلزم كذلك أن يكون الاستيلاء مادياً من قبل هذا الجاني على المال.

436 ـ ويرى جانب من الفقه[3] ان الاستيلاء الناشئ عن الاحتيال على نظام الحاسوب لا يرتب أدنى مشكلة إذا كان محل الاستيلاء نقوداً، كأن يتم التلاعب في البيانات المدخلة أو المخزنة في الحاسوب أو برامجه بواسطة شخص ما كي يستخرج الحاسوب باسمه أو باسم شركائه شيكات أو مبالغ غير مستحقة يستولي عليها الجاني مادياً أو يتقاسمها مع شركائه.

437 ـ إلاّ أن المشكلة تثار في حالة ما إذا كان محل الاستيلاء في التحايل المعلوماتي هو النقود البنكية أو الالكترونية عن طريق ما يعرف بالقيد الكتابي، فهل يعتبر هذا الاستيلاء استيلاء مادياً ومحققاً للنتيجة الإجرامية لجريمة الاحتيال ؟؟

---

(1) المصدر السابق، ص 151. وكذلك انظر، الشوا، ثورة المعلومات ... مرجع سابق، ص125.

(2) فورة، مرجع سابق، ص 583.

(3) انظر، الشوا، ثورة المعلومات ... مرجع سابق، ص 131.

438 ـ تجدر الإشارة إلى أن القيد الكتابي يتم بالتلاعب في البرامج والبيانات الأمر الذي يترتب عليه تحويل بعض الارصدة المالية أو كلها أو فوائدها من حساب أصحابها الشرعيين إلى حساب المتلاعب[1].

439 ـ ويرى البعض[2] أن العبرة في الاحتيال المعلوماتي هو بقيام الحاسوب بوضع المال محل النشاط الاجرامي تحت تصرف الجاني تحت تأثير الأساليب الاحتيالية التي مارسها الأخير، ولا يشترط أن يتم التسليم أو الاستيلاء بطريقة مادية وذلك بالمناولة اليدوية. وبالتالي فإن التحويل الالكتروني غير المشروع للأموال عن طريق عملية القيد الكتابي لا يتعارض مع مفهوم التسليم في جريمة الاحتيال التقليدية.

440 ـ وهذا ما يميل إليه جانب من الفقه المصري وكذلك الفقه الفرنسي، وهو الأمر الذي أكده كذلك القضاء الفرنسي، حيث ساوت محكمة النقض الفرنسية في بعض أحكامها بين تسليم النقود وبين الدفع الذي يتم عن طريق القيد الكتابي. فلقد ابتكرت المحكمة نظرية جديدة تعرف بإسم نظرية "التسليم المعادل" التي وضعت لمواجهة حالات الاحتيال الواقعة على ضريبة المبيعات وعلى عداد موقف السيارات وعلى الهواتف، وبعد ذلك أخذ الفقه بهذه النظرية حتى يلاحق بها أشكال النصب كلها باستخدام النظام المعلوماتي[3].

فالمحكمة عدلت عن المفهوم التقليدي لفكرة التسليم واعتبرت أن مجرد القيد الكتابي يعادل التسليم، وجاء في الحكم الذي تبنت من خلاله المحكمة هذه النظرية،[4] (.... وبالنظر إلى أن السند المثبت للانقضاء عن طريق الخصم من الدين المستحق لخزانة الدولة قد اصطنع من قبل الخاضع للضريبة، فهذا لا ينفي أحد العناصر المادية لجريمة النصب، ويظل الحال كذلك، حتى لو لم يكن هناك تسليم لنقود طالما أن الدفع تم عن طريق العملة الكتابية التي تعادل تسليم النقود....).

---

(1) الرومي، مرجع سابق، ص 64.

(2) انظر قورة، مرجع سابق، ص 478 . وكذلك، قندح، مرجع سابق، ص 12.

(3) الشوا، ثورة المعلومات ... مرجع سابق، ص 132.

(4) مشار لهذا الحكم عند، المصدر السابق، ص 133.

441 ـ أما بالنسبة لموقف تشريعات الدول المختلفة من هذه المسألة، فلقد تباينت[1]:

أولاً: اتجهت بعض الدول إلى الاعتراف للأموال الكتابية أو البنكية بصفة الأموال التي تصلح لأن تكون محلاً لجرائم السرقة والاحتيال وخيانة الأمانة بالرغم من طابعها غير الملموس. ومن هذه الدول الولايات المتحدة الأمريكية[2].

ثانياً: اتجهت دول اخرى إلى عدم اعتبار النقود البنكية أو الكتابية من قبيل الأموال المادية، بل ينظر إليها باعتبارها ديوناً لا تصلح محلاً لجرائم الاحتيال أو السرقة، كما هو الحال في التشريع الألماني والياباني.

ثالثاً: دول أخرى التزمت قوانين العقوبات فيها الصمت فيما يتعلق بهذه المسألة كما هو الحال في معظم تشريعات الدول العربية.

3- مدى امكانية اعتبار الوسائل التقنية المستخدمة في جريمة التحايل المعلوماتي من قبيل الطرق الاحتيالية التي نصت عليها المادة (417) من قانون العقوبات الاردني:

442 ـ فلقد ذهب البعض[3] ـ كما اسلفنا ـ إلى أن خداع نظام الحاسوب لسلب مال الغير تتحقق به الطرق الاحتيالية مثل كذب تدعمه أعمال مادية أو وقائع خارجية تتمثل في المعلومات أو البرامج التي يتم إدخالها إلى النظام المعلوماتي حتى تتم عملية التلاعب.

443 ـ ولكن حتى إن سلمنا باعتبار الوسائل التقنية المستخدمة في الاحتيال المعلوماتي من قبيل الطرق الاحتيالية، فإن ذلك لا يجعل تطبيق نص المادة (417) عقوبات أردني على جريمة التحايل المعلوماتي أمراً ممكناً، لأن الطرق الاحتيالية يجب

(1) انظر، الشوا، ثورة المعلومات ... مرجع سابق، ص 131،132 . وعفيفي، مرجع سابق، ص 155،156.

(2) صدرت عدة قوانين في الولايات المتحدة الأمريكية عرفت المال على انه (كل شيء ينطوي على قيمة) وهذا التعريف يشمل كافة الاموال سواء اكانت مادية ام معنوية بما في ذلك البيانات المعالجة والاموال البنكية . انظر، الشوا، ثورة المعلومات ... مرجع سابق، ص 127.

(3) المصدر السابق، ص 124.

أن تكون ابتداء في إطار العلاقات الإنسانية أي يجب أن تكون في مواجهة إنسان آخر وليس آلة وذلك وفقاً للمفهوم التقليدي لجريمة الاحتيال.

444 ـ ومما سبق يتضح لنا أن المشرع الجزائي الأردني في قانون العقوبات الأردني باعتبارها نتيجة منطقية لعجز النصوص التقليدية عن مواكبة التطور التقني الذي أبرز إلى الوجود مجموعة من الجرائم المستحدثة وعلى رأسها جريمة الاحتيال المعلوماتي، لا بد أن يقوم بالنص صراحة على تجريم هذا الفعل أو أن يقوم بتعديل النصوص القائمة بحيث تشمل في إطارها هذه الجريمة.

445 ـ وتجدر الإشارة إلى أن المشرع في قانون المعاملات الالكترونية رقم 85 لسنة 2001 اشار في المادة (35) منه على أن: (يعاقب كل من يقوم بإنشاء شهادة توثيق أو نشرها أو تقديمها لغرض احتيالي أو لأي غرض غير مشروع بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (3000) دينار ولا تزيد على (10000) دينار أو بكلتا هاتين العقوبتين). وهذه المادة تقوم على تجريم كل الأفعال الاحتيالية التي تتم باستخدام شهادة التوثيق.

والمقصود بشهادة التوثيق حسب نص المادة الثانية من ذات القانون، (الشهادة التي تصدر عن جهة مختصة مرخصة أو معتمدة لإثبات نسبة توقيع الكتروني إلى شخص معين استناداً إلى إجراءات توثيق معتمدة).

وتنص المادة (38) من ذات القانون على أن: (يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (3000) دينار ولا تزيد على (10000) دينار أو بكلتا هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون).

ونلاحظ أن هذا النص لم يراعِ العوائق التي تواجه تطبيق النصوص العقابية التقليدية في قانون العقوبات الأردني وغيره من القوانين الأخرى على الجرائم المعلوماتية، وكان من المستحسن أن يكون النص الجزائي أكثر وضوحاً وتفصيلاً لصور الجرائم المعلوماتية وذلك تماشياً مع مبدأ شرعية الجرائم والعقوبات.

المبحث الرابع
التجسس المعلوماتي

446 ـ يقول (دولف هيغل) رئيس إدارة شرطة الجرائم الخطيرة في أوروبا: (بالنسبة لجرائم الحاسوب والإنترنت، يبدو أننا قد خسرنا المعركة قبل أن نبدأ القتال.... إذ أننا لا نستطيع مجاراتها) [1]. فالحواسيب وما يرتبط بها من شبكات تبدو مثل بوابة بلا حراس، بل كساحة إجرام تتحدى الأجهزة الأمنية بثغرات قانونية ضخمة، الأمر الذي أتاح المجال أمام الأفراد والجهات الأخرى للتجول دون رقيب والحصول على المعلومات الأمنية والسرية التي قد تكون على درجة عالية من الحساسية.

447 ـ ويبدو أن شكل الحروب في الوقت الحاضر في تغير مستمر، حيث ستنتقل المعارك من ميادين القتال العادية إلى الحاسوب وشبكة الإنترنت. فالحرية المتاحة عبر الشبكة تتيح التوصل إلى المعلومات والوثائق السرية التي قد تخفيها الدول، كما أن البعض قد يتمكن من اختراق مواقع استراتيجية عسكرية وصناعية هامة لتلك الدول على الشبكة المعلوماتية أو تدمير تلك المواقع بالفيروسات.

448 ـ ويشير أحد الخبراء في هذا الصدد إلى أنه: [2] (لم تعد القوة النارية التي تمتلكها الجيوش هي وحدها التي تقرر مصير الحروب ورجحان كفة الاطراف المتقاتلة وإنما المعلومات التي يملكها كل طرف حول الطرف الآخر. وهذه الحقيقة ثابتة منذ فجر التاريخ وقد أتت التطورات السياسية والعسكرية خلال السنوات الأخيرة لتؤكدها).

فلقد أصبحت المعلومات قوة جديدة في حياة الشعوب والمؤسسات وإدارة الدولة والحكم ومن المرشح أن تصبح السيطرة على مخازن المعلومات ووسائل معالجتها في

---

(1) مناسبة هذا الحديث عقد مؤتمر لأمن الكمبيوتر في المملكة المتحدة وتحديدا في العاصمة لندن عام 2002 . انظر، الموقع الالكتروني، www.annabaa.org/nbsnews/14134.htm.

(2) انظر، عفيفي، مرجع سابق، ص 305،306.

المستقبل أكثر أهمية من الموارد الطبيعية كمصدر للقوة الاقتصادية والصناعية والعسكرية[1].

449 ـ ويمكن القول بصفة عامة أن التجسس المعلوماتي أصبح يشمل الجوانب الصناعية والتقنية والتجارية للمؤسسات الاقتصادية، كما يشمل الجوانب المتعلقة بالجانب العسكري والأمني للدولة. ولا شك أن التقدم الكبير الذي لحق بالاتصالات وصناعة الحواسيب أسفر عن ايجاد وسائل أكثر فاعلية للتجسس.

450 ـ وقد توسعت دائرة استعمال أنظمة التجسس الإلكترونية بعد أن كانت تقتصر على فئات محدودة، فالاعتقاد السائد لدى معظم الناس أن استعمال مثل هذه الأجهزة هو حكر على رؤساء الدول أو دوائر المخابرات، وأن أنظمة التجسس الوحيدة المتوفرة للأفراد هي معدات تسجيل المكالمات الهاتفية التي بالإمكان إخفائها[2].

والحقيقة أن هذا الواقع تغير أو بدأ يتغير بصورة جذرية وذلك في الدول المتقدمة صناعياً على الأقل، حيث بات بإمكان أي مستهلك شراء المعدات التي يريد إما للتجسس أو لمنع التجسس وذلك بأسعار معقولة جداً. وتجدر الاشارة إلى أن بيع وتسويق هذه الأجهزة ممنوع في معظم الدول العربية لكن ذلك لا يعني أنها غير موجودة فيها، إذ من السهل إدخالها بصورة خفية إلى هذه الدول[3].

451 ـ وللتدليل على خطورة عمليات التجسس المعلوماتي وانتشارها نشير إلى بعض الأمثلة التي حدثت في دول مختلفة من العالم[4]:

- تمكن شاب ألماني يدعى (Marcus Hess) من التجسس على أنظمة (30) حاسوب في الولايات المتحدة الأمريكية تحتوي على معلومات عسكرية

---

(1) بطرس، انطون، (1992). المعلومات وأهميتها في العصر الحديث. مجلة الكمبيوتر والاتصالات والإلكترونيات. المجلد الثامن (العدد 12)، ص38.

(2) عبده، نديم. أمن الكمبيوتر (الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي)، ط1، دار الفكر للأبحاث والدراسات، بيروت، 1991، ص 85.

(3) المصدر السابق، ص85، 86.

(4) انظر، الشوا، ثورة المعلومات.... مرجع سابق، ص 213، 214. وعفيفي، مرجع سابق، ص 307 ـ 309، وكذلك، عرب، دليل أمن المعلومات ...... مرجع سابق، ص 238 ـ 240.

وتمكن من الحصول عليها وعلى بيانات تتعلق بأبحاث علمية باستخدام طريق الاتصال البعدي.

- خسرت شركة أمريكية للبترول على مدى أشهر المناقصات التي كانت تدخل فيها، وكانت ترسو هذه المناقصات على شركة اخرى منافسة لها كانت تقدم عروض اسعار تقل فقط بضعة دولارات عن الشركة الأولى. وقد اتضح أن ذلك كان نتيجة لوجود توصيلات سرية على الحاسوب التابع للشركة التي كانت تمنى بالخسائر قامت بوضعه الشركة المنافسة لها وذلك للتعرف على عروض الاسعار المقدمة.
- تمكن أحد المبرمجين الإسرائيليين عام 1998 من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة الأمريكية وفي الكيان الصهيوني، وقد تم متابعة نشاطه من قبل المحققين في الولايات المتحدة وتم التوصل إلى الفاعل بمساعدة جهات إسرائيلية وضبطت الأجهزة المستخدمة في عملية الاختراق كلها.
- استطاع طالب ألماني نسخ بعض برامج الحاسوب على نحو غير مشروع وإفشائها، ولحقت هذه الصناعة في ألمانيا خسارة قدرت بحوالي (23) مليون مارك ألماني في الوقت الذي استفاد هذا الطالب شخصيا مبلغ (36) ألف مارك ألماني فقط.

هذه بعض الامثلة التي قمنا بعرضها لإبراز أثر التجسس المعلوماتي على الحياة الاقتصادية للدولة وكذلك على الأمن القومي والسيادة الوطنية[1].

---

(1) ناقشت الندوة التي نظمها الاتحاد العربي للمكتبات والمعلومات حول تقنية المعلومات والاتصال في الوطن العربي ـ والمنعقدة في تونس بتاريخ 18 كانون الأول 1988 ـ تعرض المواطنون العرب بحكم وضعهم الجغرافي والسياسي لجرائم التلاعب بالحاسوب بقصد التجسس والمساس بالحريات الشخصية. وكذلك تعرضت الدول العربية لمخاطر السيطرة الأجنبية في حقل إدخال أنظمة الحاسوب وتشغيلها. وخلصت الندوة إلى أن السيادة الوطنية للدول العربية معرضة للخطر إذا بقيت نظم المعلومات بعيدة عن الأيدي الوطنية، وإذا لم تنتهج سياسات وطنية وقومية لتحقيق الاكتفاء الذاتي قدر الإمكان في استخدام تقنية المعلومات. انظر، عرب، دليل المعلومات ... مرجع سابق، ص243، 244

وموضوع التجسس المعلوماتي يستدعي بيان المعلومات التي تكون هدفاً لجريمة التجسس المعلوماتي في (المطلب الأول). والوسائل التقنية المستخدمة في ارتكاب هذه الجريمة في (المطلب الثاني)، وأخيراً نلقي الضوء على مدى توافر الحماية الجنائية للمعلومات من أخطار التجسس المعلوماتي عليها في (المطلب الثالث).

المطلب الأول: المعلومات المستهدفة في جريمة التجسس المعلوماتي

452 ـ يقول الأستاذ (Ulrich Sieber) [1]: (أن الحق في المعلومات يعترف بأن المعلومات عامل اساسي ثالث بجوار الطاقة والمادة. وتنظر الأبحاث الميدانية إلى المعلومات ليس باعتبارها فقط قيمة اقتصادية وثقافية وسياسيه مستحدثة لكن بوصفها طاقة كامنة للمخاطر الاستثنائية).

453 ـ أما بالنسبة للمعلومات التي قد تكون محلاً للتجسس المعلوماتي فهي متنوعة، حتى أنها تشمل أحيانا كل ما يتعلق بحياة الدول والأفراد. وهذه المعلومات تكون على درجة من الخطورة والحيوية حيث تسعى الدول وكذلك الأفراد إلى الحصول عليها. وأبرز المعلومات التي يمكن أن تكون هدفاً لجريمة التجسس المعلوماتي تتمثل فيما يلي:

أولاً: المعلومات العسكرية

454 ـ الخطط والتدابير العسكرية وأسرار الدولة الحربية والمشروعات النووية وصناعة الأسلحة، كل هذه المعلومات التي تتعلق بالجانب الأمني والاستراتيجي للبلاد التي تعتبر أكثر المعلومات حساسية وسرية في أي دولة التي كانت توضع سابقاً في عشرات المجلدات، يمكن في الوقت الحاضر في ظل الثورة المعلوماتية تخزينها في ذاكرة الحاسوب ومعالجتها آلياً أو وضعها على قرص مغناطيسي سهل الحمل أو تحميلها على مواقع خاصة على شبكة الإنترنت.

---

(1) Sieber, ،Ulrich ، مرجع سابق، ص 53.

ويمكن في ظل هذا الوضع للمخترقين أن يقوموا باستخدام الوسائل التقنية خلال فترة زمنية قصيرة من أي مكان في العالم بالوصول إلى هذه المعلومات. بل قد يصل الأمر إلى حد تدمير هذه المعلومات العسكرية ومحوها، الأمر الذي يشكل خطراً على الأمن القومي لأي دولة.

455 ـ من أهم الحالات التي تم اكتشافها التي ارتبط فيها التجسس المعلوماتي بالمصالح العليا للدولة، تلك الحالة التي تتلخص وقائعها:[1]

بقيام ثلاثة طلبة ألمان بالعمل لحساب المخابرات السوفيتية، حيث قاموا بمدها بالشيفرات الخاصة بأنظمة حاسبات غاية في الأهمية، ومنها نظام الحاسوب الخاص بوزارة الدفاع الأمريكية (البنتاجون) ومعمل للأبحاث في (لو لاموس) وإحدى الشركات الفرنسية ومعاهد علمية متفرقة في أوروبا وأمريكا الشمالية واليابان.

وتمكن الجناة في هذه الواقعة من الدخول إلى أنظمة الحاسبات سالفة الذكر عبر شبكات المعلومات وتمكنوا من استغلال بعض الثغرات التي تعتري الإجراءات الأمنية لهذه الأنظمة للحصول على الشيفرات الخاصة بها.

ولقد تم اكتشاف الجناة بالصدفة، واستغرقت عملية تتبعهم عاماً كاملاً قدموا بعده للمحاكمة أمام القضاء الألماني ووجهت اليهم تهمة التجسس لصالح دولة اجنبية وكان ذلك في عام 1989.

456 ـ وتبدو خطورة وحساسية المعلومات العسكرية والأمنية للدولة اذا علمنا أن البنتاغون يقوم بتغيير أنظمة الترميز السرية لبياناته ولمعلوماته الحساسة يومياً، كما أنه ينفق على أحد برامجه (200) مليون دولار كل سنة ويقوم هذا البرنامج بإلغاء وكتم الإشارات الصادرة من الآلات المستخدمة بواسطة العسكريين ووكالات الأمن ومتعهدي الدفاع [2].

(1) مشار لهذه الواقعة، قورة، مرجع سابق، ص 280.

(2) فوريستر، مرجع سابق، ص 408.

457 ـ وكان كتاب قد صدر في باريس تحت عنوان (عين واشنطن) قد كشف عن قيام جهازي المخابرات الأمريكية والإسرائيلية باختراق جميع أجهزة الحاسوب في العالم بهدف الحصول على جميع المعلومات المتعلقة بالدول الأخرى في المجالات كلها.

وأشار الكتاب إلى أن الولايات المتحدة الامريكية تقوم بعمل كمائن للنظم المعلوماتية لدى أعدائها وحلفائها على حد سواء، بحيث تصبح لديها جميع المعلومات في مختلف المجالات[1].

وقد أكد الكتاب كذلك وجود ما يسمى بمركز المعلومات الكوني الذي تودع فيه المعلومات التي يتم تجميعها عبر نظم معلوماتية خاصة تم ترويجها وبيعها في العالم، وفي النهاية هي تعمل في خدمة وكالة المخابرات الامريكية (CIA) والموساد الإسرائيلي[2].

ثانياً: المعلومات الاقتصادية

458 ـ يقول القاضي الفرنسي (Louis Joinet): (إن المعلومات قوة اقتصادية والقدرة على تخزين أنواع معينة من البيانات ومعالجتها، يمكن أن يعطي بلداً مميزات أساسية وتكنولوجية على البلدان الاخرى.....)[3].

459 ـ مما لا شك فيه إن الاقتصاد يعتبر من العوامل الرئيسية في سيادة مختلف الدول وأمنها وتهدف أعمال التجسس على المعلومات التجارية والصناعية والمالية إلى معرفة الثغرات الاقتصادية في دولة ما ومواطن الضعف في هيكلها الاقتصادي وكذلك يهدف إلى التفوق اقتصادياً على تلك الدولة. كما أن التجسس المعلوماتي قد يتم على المستوى الداخلي بين المؤسسات الاقتصادية المختلفة في ذات الدولة.

460 ـ كانت التوصية الصادرة عن المجلس الاوروبي الخاصة بجرائم الحاسوب قد عرفت المعلومات الصناعية والتجارية السرية أنها: (مجموعة من الحقائق لها قيمة معلوماتية ولها صلة بشخص او بمؤسسة محددة وتتميز هذه الحقائق بكونها سرية، أي

(1) عفيفي، مرجع سابق، ص 311.

(2) المصدر السابق، ص311، 312.

(3) انظر، عرب، امن المعلومات ... مرجع سابق، ص 244.

غير معلومة للجميع، وأن الدخول إلى الأنظمة التي تحتوي عليها مقصور على دائرة محددة من الاشخاص، وتظل هذه السرية رهناً بإرادة الشخص المسؤول عن المؤسسة[1].

461 ـ والتجسس المعلوماتي في النطاق التجاري يسعى للحصول على الأسرار التسويقية والحسابات المالية للمؤسسة المستهدفة بعملية التجسس، وكذلك معرفة المعلومات الكافية حول حساب التكلفة وكشف الميزانية وحالة الاسواق والعناوين الخاصة بالعملاء، وكذلك معرفة تنقلات الاموال والاستثمارات في المنشآت العامة أو الخاصة[2].

462 ـ أما فيما يتعلق بالتجسس المعلوماتي في النطاق الصناعي، فيهدف إلى الكشف عن أسرار الانتاج للصناعات المختلفة، بما في ذلك معرفة خطوات الانتاج وكذلك التوصل إلى الأبحاث العلمية التي تجري لتطوير الصناعات المختلفة.

463 ـ والحاجة إلى توفير سنوات عديدة من البحث العلمي الشاق وتجنباً لاستثمار ملايين الدولارات في هذه العمليات قد تدفع المؤسسات المختلفة بل حتى الدول إلى اللجوء لأسلوب التجسس المعلوماتي من أجل الحصول على الأسرار الصناعية دون تحمل الأعباء المادية.

ويبدو ذلك بشكل واضح في مجال صناعة برامج الحاسوب، حيث أن صناعة هذه البرامج عادة ما تكلف مبالغ باهظة بالإضافة إلى الوقت الذي تستغرقه والأبحاث اللازمة لذلك. وقد كان ذلك سبباً وراء لجوء الكثير من الشركات للتجسس للحصول على المعلومة الخاصة بإنتاج هذه البرامج، إما لإنتاج برامج مماثلة وتسويقها أو لزيادة الخبرة في هذا المجال أو لمجرد التعرف على ما توصلت إليه شركة منافسة[3].

464 ـ هناك دراسة تشير إلى أن ثلث الشركات الأوروبية تتعرض لنوع من أنواع البرامج التجسسية من نوع (Spware)[4]. ومن الوقائع التي أظهرت خطورة هذا النوع من

---

(1) انظر، قورة، مرجع سابق، ص281.

(2) عبده، مرجع سابق، ص49. وكذلك، شتا، مرجع سابق، ص 94.

(3) قورة، مرجع سابق، ص 280.

(4) انظر الموقع الالكتروني، www.gn4me.com/etesalat/article.jsp.

التجسس ما كشف عنه في ربيع (1990) من أن مكتب التحقيقات الفيدرالي الأمريكي (FBI) ووكالة الاستخبارات المركزية (CIA) ألقت القبض على أعضاء في جهاز الاستخبارات الفرنسية، بعد أن ضبطوا متلبسين بجريمة التجسس على أكبر شركات الحاسوب الأمريكية وخصوصاً شركتي (IBM) و(Texas Instruments) ويذكر أن الجواسيس الفرنسيين كانوا قد تمكنوا من الدخول إلى قواعد البيانات الخاصة بالمعلومات الداخلية للشركتين وذلك بغية الكشف عن خططهما وأسرارهما الصناعية[1].

وتعكس هذه القضية - التي لا تعتبر قضية فريدة من نوعها - الدور المتعاظم الذي بات يلعبه الحاسوب في قطاع الجاسوسية والأهمية التي تعلقها دوائر المخابرات لاكتشاف الأسرار الصناعية الحاسوبية.

ثالثاً: البيانات السكانية والاجتماعية

465 ـ يتم جمع البيانات المتعلقة بالاحصاءات السكانية وكذلك المعلومات المتعلقة بالوضع الاجتماعي للسكان من حيث ديانتهم واصولهم ومستوى المعيشة الخاص بهم وكذلك نسبة الذكور إلى الاناث في الدولة والتوزيع الجغرافي للسكان وغير ذلك من المعلومات والتي تبني عليها الدولة خططها التنموية و الاقتصادية.

466 ـ وبعد انتهاء عملية جمع هذه المعلومات يتم عادة في معظم الدول تخزينها في ذاكرة الحاسوب على مواقع خاصة تابعة للدولة التي تتعلق هذه البيانات بسكانها، ومن ثم تتم معالجة هذه المعلومات آلياً بغية الاستفادة منها في تحقيق الاهداف المنشودة في الدولة.

إلاّ أن هذه البيانات والمعلومات قد يتم اساءة استعمالها والتجسس عليها من قبل جهات قد تكون داخلية، أي من داخل الدولة ولأغراض خاصة بها أو من قبل جهات خارجية، أي من قبل دولة معادية تهدف لمعرفة الجوانب المختلفة لدولة ما لتحقيق أهداف خاصة بها. ومن الأمثلة على التجسس على هذا النوع من البيانات[2]:

---

(1) انظر، عبده، مرجع سابق، ص49.

(2) عفيفي، مرجع سابق، ص 312.

- قيام موظفين من العاملين بمركز حاسوب في السويد بنسخ برامج مسجل عليها احصاءات وبيانات سكانية، حيث قاما ببيعها بعد ذلك إلى أحد المكاتب الخاصة بالاحصاءات والبيانات لأغراض استهلاكية مقابل ثمن رخيص.

المطلب الثاني: الوسائل التقنية المستخدمة في التجسس المعلوماتي

467 - تطورت أساليب التجسس المعلوماتي مواكبة التطور الذي يشهده العالم، خاصة في مجال تكنولوجيا المعلومات والاتصالات. حيث لم يعد التجسس مقتصراً على تجنيد عملاء في الدول الأخرى للحصول على المعلومات العسكرية أو الدفاعية لهذه الدول من قبل دول معادية لها، أو تجنيد هؤلاء العملاء في المؤسسات التجارية والصناعية المختلفة بهدف التوصل إلى أسرار هذه المنشآت، أو اللجوء إلى رشوة العاملين وابتزازهم في هذه المؤسسات للحصول على المعلومات الحساسة فيها.

فالتقنية الرقمية فتحت آفاقاً واسعة للقيام بالتجسس دون حاجة لاختراق الدول والمؤسسات المختلفة من قبل عناصر بشرية، بل يمكن للجهات الحصول على ما تريد من المعلومات الحساسة والخطيرة عن بعد.

468 - والوسائل التقنية في مجال تكنولوجيا المعلومات التي تستخدم في التجسس المعلوماتي كثيرة ويصعب حصرها، إذ أنها متطورة باستمرار وهناك سعي وبحث دائم من قبل بعض الجهات والدول للوصول إلى مرحلة متقدمة في مجال صناعتها. ويمكن الإشارة في هذا الصدد إلى أبرز هذه الوسائل التقنية التي تتمثل في:

أولاً: استعمال هوائيات مع ربطها بحاسوب خاص[1]

469 - وتستخدم هذه التقنية للتجسس على المعلومات في حال تخزينها في جهاز الحاسوب، حيث يمكن عن طريق هذه الهوائيات التقاط الموجات الكهرومغناطيسية المنبعثة من الحاسوب خلال فترة تشغيله مع إمكانية تسجيلها ومعالجتها وترجمتها إلى

(1) انظر، عفيفي، مرجع سابق، ص 313.

معلومات تتسم بالوضوح.حيث يمكن أن يتم التقاط المعلومات من مسافة تزيد على ثلاثمائة قدم من الحاسوب المستهدف.

ثانياً: استعمال تقنية أبواب المصيدة (Trap Doors) [1]

470 ـ وتسمى أيضاً تقنية الأبواب الخفية. ويقوم عمل هذه التقنية على ترك ثغرات تسمح بالدخول إلى البرنامج مرة أخرى عند اعداده وذلك لتلافي ما قد يرد فيه من أخطاء.

وهذه الثغرات من المفروض أن يتم الغاؤها في النسخة النهائية للبرنامج إلاّ أنه قد يتم تركها عمداً وبذلك يكون من الممكن لأي شخص إذا وجد هذه الأبواب أن يتوصل إلى المعلومات في جهاز الحاسوب.

ثالثاً: الاعتراض للمعلومات المنقولة عبر النظام المعلوماتي

471 ـ تقوم هذه التقنية على معرفة محتوى اتصال قد يتم داخل نظام حاسوب واحد، أو بين نظامين مختلفين أو بين عدة أنظمة ترتبط فيما بينها من خلال شبكة اتصالات وذلك بالتقاط المعلومات التي يتضمنها هذا الاتصال.

472 ـ والتقاط الموجات الكهربائية الصادرة عن النظام المعلوماتي تعد الوسيلة الاساسية لاعتراض المعلومات المتنقلة عبر النظام. فمن خلال هذه الوسيلة يمكن جمع المعلومات عن بعد. حيث من الممكن ـ على سبيل المثال ـ جمع معلومات يتم إرسالها من خلال نظام حاسوب داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى. وتقوم هذه الشاشة بالتقاط الموجات الكهربائية التي تحيط بالحاسوب التي تتحول إلى معلومات مقروءة على الشاشة من ناحية، كما يتم تسجيلها من ناحية اخرى[2].

كما يمكن استخدام أجهزة التقاط خاملة لا تصدر أية اشارات لاسلكية لاعتراض وصلات الموجات القصيرة التي تحتوي على مجموعة من القنوات المحتوية على

(1) انظر، المصدر السابق، ص313.

(2) قورة، مرجع سابق، ص 363، 364.

بيانات، حيث يمكن بهذه الطريقة اعتراض ما يجري من اتصالات بين المحطات الارضية والاقمار الصناعية[1].

رابعاً: التوصيل المباشر على خط تليفوني

473 ـ وتباشر هذه التقنية عملها عن طريق وضع مركز تصنت يسهل تسجيل كل الاتصالات كما يمكن أن تؤدي هذه الوظيفة ميكروفونات صغيرة[2].

474 ـ وتجدر الإشارة إلى أن عملية التصنت على المكالمات الهاتفية كانت من الأمور السهلة سابقاً، حيث كان يكفي تركيب ما يعرف بملقط التمساح (Alligator Clip) على خطوط الاتصال للاستماع إلى المخابرات التي تتم عبر الخطوط.

إلاّ أن الأمر تغير الآن مع تزايد الاعتماد على التقنية الرقمية عبر شبكات الاتصالات الهاتفية، حيث أن الخطوط الرقمية تنقل آلاف المخابرات في وقت واحد وبعد ذلك تجري تجزئتها أثناء عملية النقل ليعاد جمعها أو ضمها عند الطرف المستقبل، حيث أن تركيب ملقط كما في السابق لا يجدي نفعاً لمعرفة محتوى الاتصالات نظراً إلى أن البيانات التي يمكن التقاطها ستكون مشتتة بين عدة مخابرات وبالتالي فانها لا تعني شيئاً[3].

خامساً: إدخال ملف تجسس إلى جهاز الحاسوب الخاص بالمجني عليه

475 ـ وفي حالة إصابة الجهاز بملف التجسس يقوم على الفور بفتح أحد المنافذ في جهاز الجهة المجني عليها، وهذا المنفذ هو الباب الخلفي لحدوث اتصال بين جهاز الشخص المجني عليه وجهاز المخترق. والملف الذي يكون لدى المجني عليه يسمى الخادم، بينما الجزء الآخر منه يسمى العميل ويكون لدى المخترق الذي من خلاله

---

(1) عفيفي، مرجع سابق، ص 314.

(2) الشوا، ثورة المعلومات ... مرجع سابق، ص 69.

(3) التصنت على الاتصالات التي تعتمد التقنية الرقمية. (1995) . مجلة الكمبيوتر والاتصالات والإلكترونيات. المجلد (12) العدد (7) ص55 .

يمكن للشخص أو الجهة التي تقوم بعملية التجسس أن تسيطر على جهاز المجني عليه دون أن يشعر الأخير بذلك[1].

476 ـ ويتم إدخال ملف التجسس إلى جهاز المجني عليه عن طريق ثلاث طرق غالباً[2]:

الطريقة الأولى: من خلال برامج المحادثة على شبكة الإنترنت حيث يقوم الشخص أو الجهة التي تريد القيام بعملية التجسس بإرسال ملف للمجني عليه وتؤكد على احتوائه على أمور تهمه ويكون ذلك الملف هو ملف التجسس.

الطريقة الثانية: وتكون من خلال البريد الالكتروني للشخص أو الجهة المجني عليها ، حيث يتم إرسال رسالة الكترونية إلى المجني عليه فيقوم بفتحها فإذا بها تحتوي على ملفات ملحقة تحمل برنامج التجسس.

الطريقة الثالثة: تكون عند زيارة الشخص أو الجهة المجني عليها لمواقع مجهولة. وتقوم هذه المواقع بإغراء الزائرين بتنزيل بعض البرامج والملفات المجانية ومن ضمنها ملف التجسس.

477 ـ وتجدر الإشارة إلى أن الدول والجهات المختلفة لجأت إلى استحداث وسائل تقنية في سبيل حماية معلوماتها وبياناتها ، ومن أبرز هذه الطرق:

1- تشفير البيانات:

478 ـ المقصود بتشفير البيانات: كتابتها برموز سرية يتعذر معها على كل من لا يحوز مفتاح تلك الشيفرة أن يخترق شبكة المعلومات.

وتجدر الاشارة إلى أن أنظمة التشفير لا توفر الحماية الكافية إذ يمكن حلها في زمن طال أم قصر، وفي هذا المجال يؤكد الأستاذ (Parker) على أنه: (يمكن لأي

(1) الرومي، مرجع سابق، ص 136.

(2) المصدر سابق، ص 137.

حكومة تتوافر لديها الامكانيات الفنية تصميم حاسوب بالغ القوة يتيح لها فك أية شيفرة أمكن تصميمها ومن ثم كشف أسرار أيه منظمة تختارها)[1].

2- استخدام اجهزة التشويش الإلكتروني[2]:

479 ـ حيث تقوم هذه الأنظمة بتحويل الاتصالات الهاتفية أو البيانية إلى تداخلات غير مفهومة لا يمكن فكها إلاّ بواسطة كود خاص. وهناك أيضا أنظمة الخداع، التي تجعل المتجسس ينخدع لجهة الأصوات التي يعتقد أنه يلتقطها.

3- استخدام كلمة سر:

480 ـ والمقصود بذلك استخدام رقم أو كلمة رمزية سرية لا يمكن التعامل مع النظام المعلوماتي سواء أكان من نهاية طرفية معينة او لإدخال بيانات معينة الا بذكرها.

ومن الأفضل تغيير كلمات السر بصورة دورية لتجنب إمكانية الاطلاع عليها من قبل أشخاص غير مسموح لهم بذلك[3].

4- استخدام أجهزة القياس الحيوي أو الاجهزة البيومترية[4]:

481 ـ وهذه الأجهزة لا تسمح بالوصول إلى النظام المعلوماتي إلاّ لأشخاص مصرح لهم بذلك، ويتم ذلك بعد التعرف عليهم بواسطة هذه الأجهزة عن طريق ما يتم تخزينه من خصائص طبيعية عضوية ينفرد بها الشخص عن غيره، مثل بصمات الأصابع ومقاسات الكف وتحليل نبرات الصوت وديناميكية التوقيع المعتمدة على حركة أداة الكتابة والزمن الذي تستغرقه الحركات أو الضربات اللازمة لإنهاء التوقيع كاملاً.

---

(1) عفيفي، مرجع سابق، ص317.

(2) انظر، عبده، مرجع سابق، ص87.

(3) عفيفي، مرجع سابق، ص315.

(4) انظر، المصدر السابق، ص 316، 317 وكذلك، شتا، مرجع سابق، ص96.

وأخيراً لا بد أن نشير إلى أن الخبراء المختصين بأمن النظم المعلوماتية يؤكدون أن وسائل الحماية الفنية المعروفة كلّها الآن قد فشلت في تحقيق الأمن للنظام المعلوماتي وبياناته وبرامجه.

ويفسر أحدهم ذلك بقول شائع مفاده: (إن ما يستطيع انسان انشاءه يمكن للآخر تقويضه).

المطلب الثالث: الحماية الجنائية للمعلومات من خطار التجسس المعلوماتي

482 ـ نص المشرع الجزائي الأردني في قانون العقوبات على جريمة التجسس في الفصل الأول من الباب الأول تحت عنوان "في الجرائم التي تقع على أمن الدولة"، وذلك في المواد (124 ـ 126).

وقد بيّن المشرع على أن هذه المواد قد ألغيت بموجب قانون حماية أسرار ووثائق الدولة رقم (50) لسنة (1971).

483 ـ ويثار التساؤل حول مدى الحماية التي يوفرها هذا القانون للمعلومات والبيانات الحساسة ـ العسكرية أو التجارية أو الصناعية منها التي يشكل المساس بها مساساً بأمن الدولة واستقرارها ـ من أخطار التجسس المعلوماتي الذي يتم بأحدث الوسائل والتقنيات الرقمية.

484 ـ نشير ابتداء إلى أن قانون حماية أسرار الدولة ووثائقها عرف في المادة الثانية منه الأسرار والوثائق المحمية أنها:

(أية معلومات شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو ورق مشمع أو ناسخ أو أشرطة تسجيل أو الصور الشمسية والأفلام أو المخططات أو الرسوم أو الخرائط أو ما يشابهها والمصنفة وفق أحكام هذا القانون).

وهذا التعريف واسع فضفاض، من الممكن أن يشمل المعلومات المخزنة في جهاز الحاسوب ونظامه المعلوماتي، حيث أشار التعريف إلى أن الأسرار والوثائق المحمية تشمل المعلومات والوثائق المختزلة.

485 ـ وقد بينت المواد (3، 6، 8) من القانون ذاته طبيعة المعلومات التي تشكل أسراراً يجب عدم المساس بها نظراً لخطورتها وأهميتها ولقد تدرجت هذه المواد من المعلومات التي تشكل غاية السرية إلى المعلومات التي تعتبر محدودة السرية.

حيث نصت المادة الثالثة من هذا القانون على أنه: (تصنف بدرجة سري للغاية أية أسرار أو وثيقة محمية إذا تضمنت الأمور التالية:

1- أية معلومات يؤدي إفشاء مضمونها لأشخاص تقتضي طبيعة عملهم الاطلاع عليها أو الاحتفاظ بها أو حيازتها إلى حدوث أضرار خطيرة بأمن الدولة الداخلي أو الخارجي أو إلى فائدة عظيمة لأية دولة أخرى من شأنها أن تشكل أو يحتمل أن تشكل خطراً على المملكة الأردنية الهاشمية.
2- خطط وتفصيلات العمليات الحربية أو اجراءات الأمن العام أو المخابرات العامة أو أية خطة ذات علاقة عامة بالعمليات الحربية أو اجراءات الأمن الداخلي سواء أكانت اقتصادية انتاجية أو تموينية أو عمرانية أو نقلية.
3- الوثائق السياسية الهامة جداً ذات الخطورة المتعلقة بالعلاقات الدولية والاتفاقات أو المعاهدات وكل ما يتعلق بها من مباحث ودراسات.
4- المعلومات والوثائق المتعلقة بوسائل الاستخبارات العسكرية أو المخابرات العامة أو الاستخبارات المعاكسة أو مقاومة التجسس أو أية معلومات تؤثر على مصادر الاستخبارات العسكرية والمخابرات العامة أو المشتغلين فيها.
5- المعلومات الهامة المتعلقة بالأسلحة والذخائر أو أي مصدر من مصادر القوة الدفاعية التي يشكل افشاؤها خطراً على أمن الدولة الداخلي أو الخارجي).

ونصت المادة السادسة من القانون ذاته أنه: (تصنف بدرجة سري أية أسرار أو وثيقة محمية لم تكن من درجة سري للغاية إذا تضمنت المعلومات التالية:

1- أية معلومات هامة يؤدي إفشاء مضمونها لأشخاص لا تقتضي طبيعة عملهم الاطلاع عليها إلى تهديد سلامة الدولة أو تسبب إضراراً لمصالحها أو تكون ذات فائدة كبيرة لأية دولة أجنبية او أية جهة اخرى.

2- أية معلومات عن مواقع تكديس المواد الدفاعية أو الاقتصادية أو المؤسسات الحيوية المتعلقة بمصادر القوة متى كان لها مساس بسلامة الدولة.

3- أية معلومات عن تحركات القوات المسلحة أو الأمن العام.

4- أية معلومات عن أسلحة وقوات الدول العربية الشقيقة).

وكذلك تضمنت المادة الثامنة من قانون حماية أسرار الدولة ووثائقها المعلومات أو الوثائق التي تصنف بدرجة (محدود)[1].

486 ـ بين المشرع الجزائي الأردني في القانون ذاته وفي المواد (12 ـ 16)[2] السلوكيات التي يقع بها الركن المادي لجرائم التجسس. ويبدو من نصوص هذه المواد

---

(1) نصت هذه المادة على أنه: (تصنف بدرجة محدود أية معلومات أو وثائق محمية تتضمن معلومات تنطبق عليها الأوصاف التالية:

1- أية معلومات يؤدي افشاؤها إلى أشخاص غير مصرح لهم بالاطلاع عليها إلى اضرار بمصالح الدولة أو يشكل حرجاً لها أو ينجم عنه صعوبات إدارية أو اقتصادية للبلاد او ذات نفع لدولة اجنبية أو اية جهة اخرى قد يعكس ضرراً على الدولة.

2- اية وثائق تتعلق بتحقيق إداري او جزائي او محاكمات او عطاءات أو شؤون مالية او اقتصادية عامة ما لم يكن إفشاء مضمونها مسموحاً به.

3- تقارير الاستخبارات العسكرية ما لم تكن داخلة ضمن تصنيف آخر من درجة أعلى .

4- التقارير التي من شأن إفشاء مضمونها إحداث تأثير سيء على الروح المعنوية للمواطنين ما لم يؤذن بنشرها.

5- موجات اللاسلكي العسكرية التابعة للقوات المسلحة والامن العام والمخابرات العامة او اية سلطة حكومية أخرى.

6- اية معلومات أو وثيقة محمية تضر بسمعة أية شخصية رسمية او تمس هيبة الدول).

(2) تنص المادة 12 من قانون حماية اسرار الدولة ووثائقها على أنه (يحظر على أي مسؤول تخلى عن وظيفته بسبب النقل او إنهاء الخدمة او لأي سبب آخر افشاء اية معلومات او اسرار حصل عليها أو عرفها بحكم وظيفته وكان إفشاؤها محظوراً وفق احكام هذا القانون). وتنص المادة 13 على أنه (يحظر اخراج الوثائق المحمية من الدوائر الرسمية ما لم تكن الضرورة قد اقتضت ذلك ويمنع الاحتفاظ بها في المساكن والأماكن العامة ويحظر طباعة أو نسخ الوثائق المحمية خارج الدوائر الرسمية) . وتنص المادة 14 على أن: (من دخل او حاول الدخول إلى مكان محظور قصد الحصول على أسرار أو اشياء او وثائق محمية أو معلومات يجب أن تبقى سرية حرصاً على سلامة الدولة عوقب بالأشغال الشاقة المؤقتة وإذا حصلت هذه المحاولة لمنفعة دولة اجنبية عوقب بالأشغال الشاقة المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام) . وتنص المادة 15 على أن: (من سرق اسرار او اشياء او وثائق او معلومات كالتي ذكرت في المادة السابقة أو استحصل عليها عوقب بالأشغال الشاقة المؤقتة لمدة لا تقل عن عشر سنوات) . وتنص المادة 16 من القانون ذاته على أن (من وصل إلى حيازته او علمه اي سر من الأسرار او المعلومات او اية وثيقة محمية بحكم وظيفته او كمسؤول او بعد تخليه عن وظيفته او مسؤوليته لأي سبب من الأسباب فابلغها او افشاها دون سبب مشروع عوقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات) .

ان التجسس المعلوماتي الذي يتم بالوسائل التقنية الحديثة كان غائباً عن ذهن المشرع، والسبب الرئيسي في ذلك هو أن التجسس في وقت إعداد هذا القانون وإقراره كان يتم بالطرق المباشرة، حيث لا بد من الوصول إلى هذه المعلومات والوثائق من قبل أحد العناصر البشرية من داخل المنشأة أو خارجها.

بعكس ما هو عليه الحال في الوقت الراهن فبالامكان الحصول على هذه المعلومات على بعد آلاف الكيلو مترات باستخدام التقنيات الرقمية.

487 ـ في الواقع إن محاولة تطويع نصوص هذه المواد لتشمل في طياتها جريمة التجسس المعلوماتي القائمة على التكنولوجيا الرقمية تتعارض مع مبدأ جوهري وأساسي ألا وهو شرعية الجريمة والعقوبة وحظر القياس في القانون الجنائي، حتى في الحالة التي يتم فيها مد بعض هذه النصوص لتشمل بعض الأفعال المكونة لجريمة التجسس المعلوماتي ـ كما هو الحال في المادتين 15 و16 من القانون ذاته ـ فإن الأمر الذي لا شك فيه أن هناك افعالاً أخرى سوف تخرج من نطاق التجريم لصعوبة وضعها تحت نص تقليدي.

ومن هنا فإننا نجد أنه لا بد من تدخل المشرع الجزائي الأردني لتعديل أو إضافة نصوص قانونية تنص صراحة على تجريم التجسس المعلوماتي وتحديد الركن المادي الذي تقوم به هذه الجريمة، خاصة ونحن ندرك مدى خطورة وحساسية المعلومات محل جريمة التجسس على الأمن الداخلي والخارجي للدولة.

488 ـ وكذلك فإن التعاون الدولي في مجال مكافحة التجسس المعلوماتي مطلب اساسي، لا بدّ أن يتزامن مع تعديل التشريعات الداخلية. فهذه الجريمة شأنها شأن سائر جرائم المعلوماتية متعدية للحدود والقارات.

489 ـ ولقد قامت العديد من الدول بإصدار قوانين خاصة تجرم التجسس المعلوماتي ونذكر على سبيل المثال:

- الولايات المتحدة الامريكية التي تم فيها إصدار قانون التجسس الاقتصادي في عام (1996)، حيث أصبحت بموجبه هذه الجريمة من

الجرائم الفيدرالية. ووفقاً لهذا القانون يمنع الولوج الى أي نظام معلوماتي للحصول على معلومات مملوكة للغير.

كما أن قانون إساءة استخدام الحاسوب الصادر في عام (1984)، وفي الفقرة (أ) من المادة (1030) نص على[1]:

(معاقبة كل من اتصل عن علم دون تصريح بحاسوب و انتهز ذلك لتحقيق أغراض خارج نطاق التصريح المخول له وتمكن بهذا السلوك من:

1- الحصول على معلومات سرية لحكومة الولايات المتحدة الامريكية بقصد استخدامها أو بسبب الاعتقاد في إمكانية استخدامها للإضرار بالولايات المتحدة أو لفائدة دولةأاجنبية.

2- الحصول على معلومات تتعلق بمؤسسة مالية أو بوكالة تقدم تقارير عن المركز الائتماني للمستهلكين.

3- استخدام أو تعديل أو اتلاف أو تدمير او إفشاء معلومات مخزنة في حاسوب أو منع الاستخدام المصرح به لحاسوب متى كان هذا الحاسوب يعمل أو يدار لأجل أو بالنيابة عن حكومة الولايات المتحدة الأمريكية وكان من شأن سلوك الفاعل التأثير في تشغيله.

- وتعاقب المادة (370/ب) من قانون العقوبات اليوناني[2]:

كل من يقوم على نحو غير مشروع بنسخ معلومات مبرمجة أو طباعتها أو استعمالها أو إفشائها أو برامج للحاسوب تحتوي على أسرار تتعلق بالدولة، أو أسرار علمية أو أسرار مهنية أو أسرار تتعلق بالمؤسسات الاقتصادية في القطاعين الخاص والعام، أو اعتدى بأية وسيلة أخرى على مثل هذه المعلومات.

وتشدد العقوبة متى كان الفاعل من العاملين لدى الجهة المعنية بهذه المعلومات والبرامج أو إذا كانت لهذه المعلومات قيمة اقتصادية مرتفعة.

---

(1) انظر، عفيفي، مرجع سابق، ص 323.

(2) قورة، مرجع سابق، ص 282.

490 ـ وتجدر الاشارة إلى أن المجلس الأوروبي قد دعا في توصيته الخاصة بجرائم الحاسوب الدول الأعضاء في المجلس إلى تجريم التجسس المعلوماتي عند مراجعة قوانينها العقابية وتحديداً التجسس المتعلق بالمعلومات الصناعية والتجارية.

ولقد اقترح المجلس الأوروبي نصاً يمكن الاسترشاد به عند تجريم التجسس المعلوماتي. ووفقاً لهذا النص يتم تجريم[1] (الحصول بوسائل غير مشروعة أو الافشاء أو النقل أو الاستعمال لمعلومات صناعية أو تجارية ذات طابع سري، دون وجه حق أو دون أي مبرر قانوني آخر، على أن يكون ذلك بنية إلحاق خسارة اقتصادية للشخص المعني بهذه المعلومات أو الحصول على مكاسب اقتصادية غير مشروعة للفاعل أو لغيره).

(1) انظر، المصدر السابق، ص 281.

الخاتمة

491 ـ أصبحت المعلوماتية سمة العصر وبات استخدام الأنظمة المعلوماتية من قبل الدول والأفراد المقياس الذي يحدد مدى تطور الشعوب وتقدمها. فتكنولوجيا المعلومات تساهم في تسريع إنجاز الأعمال، الأمر الذي يعني تنفيذ الأهداف والخطط التي ترسمها الدول لتحقيق التنمية الاقتصادية والاجتماعية والسياسية في وقت قياسي. ومن هنا أصبح لزاماً على الدول من أجل ضمان نهضتها وتماشياً مع عصر المعلوماتية الذي لا ينتظر أحداً أن تعمل على مواكبة التطور التكنولوجي والالكتروني الذي نجم عن تحول العديد من المجتمعات إلى مجتمعات معلوماتية تعتمد على التقنية الرقمية في أداء أعمالها.

492 ـ إلاّ أن عصر المعلوماتية خلف ورائه آثاراً سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الغرض الذي خلقت من أجله، الأمر الذي أثر على حقوق الأفراد وحرياتهم حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم، كما أضحى النظام المعلوماتي ذاته محلاً للاعتداء عليه وإساءة استخدامه.

493 ـ ولقد ألقى هذا التطور التكنولوجي المعلوماتي مسؤولية كبيرة على عاتق المشرع الجنائي لمواجهة الجرائم المعلوماتية الناشئة عن إساءة استخدام الأنظمة المعلوماتية خاصة في ظل قصور نصوص قانون العقوبات عن الإحاطة بهذه الجرائم لأن قواعده وضعت ابتداء لحماية الأموال ذات الطبيعة المادية الملموسة التي لها كيان في الفضاء الخارجي الأمر الذي يتعذر معه حماية القيم غير المادية المتولدة عن المعلوماتية.

494 ـ وخلال هذه الدراسة المتواضعة كنا قد عرضنا في الفصل التمهيدي نبذة عن الجانب الفني والتقني للنظام المعلوماتي.

ومن ثم تناولنا في الفصل الأول تعريف الجريمة المعلوماتية والسمات الخاصة التي تتميز بها ووجدنا أنها جرائم عابرة للحدود ويصعب اكتشافها وإثباتها كما أنها تتم بأسلوب لا يتسم بالعنف وتتم عادة بتعاون أكثر من شخص، ثم بحثنا بعد ذلك في

دواعي الحماية الجنائية للمعلوماتية ووجدنا أن توجه الأردن نحو مشروع الحكومة الالكترونية والخسائر الفادحة التي قد تتسبب بوقوعها الجرائم المعلوماتية وقصور التشريعات القائمة عن الإحاطة بجوانب هذه الجرائم، هي من أهم الأسباب التي تدعو إلى هذه الحماية. ثم عرضنا بعد ذلك للمجرم المعلوماتي سماته وطوائفه ودوافعه إيماناً منا أن دراسة شخصية المجرم تساهم في وضع التشريعات الجنائية التي تكفل ردعه وإصلاحه في ذات الوقت.

ثم تناولنا في الفصل الثاني أبرز الجرائم المعلوماتية التي يكون النظام المعلوماتي فيها محلاً للاعتداء وتناولنا تحديداً الجرائم التي تقع على الشق المعنوي لهذا النظام وهذه الجرائم هي سرقة المعلومات والاستعمال غير المصرح به للنظام المعلوماتي وجريمة إتلاف المعلومات وجريمة التزوير المعلوماتي، ووجدنا أن النصوص التقليدية في قانون العقوبات الأردني قاصرة عن شمول هذه الجرائم ضمن نطاقها.

أما الفصل الثالث والأخير فبحثنا فيه الجرائم المعلوماتية التي تقع بواسطة النظام المعلوماتي وهي الدخول والبقاء غير المصرح بهما داخل النظام المعلوماتي والاعتداء على حرمة الحياة الخاصة للأفراد والاحتيال المعلوماتي وجريمة التجسس المعلوماتي، ووجدنا أن قانون العقوبات الأردني يخلو من أي نص يجرم أو يشير إلى فعل الدخول والبقاء غير المصرح بهما داخل النظام المعلوماتي، أما باقي الجرائم فوجدنا أنه من الصعوبة بمكان أن تشملها النصوص التقليدية في قانون العقوبات الأردني.

495 ـ واستناداً إلى ما سبق وبناءً على المبدأ القانوني الجوهري في القانون الجنائي ألا وهو مبدأ شرعية الجريمة والعقوبة وعدم جواز القياس في النصوص الجزائية فإننا نخلص إلى التوصيات التالية:

- ضرورة تدخل المشرع الجزائي الأردني لاستحداث نصوص قانونية في قانون العقوبات تحت اسم (الجرائم المعلوماتية) تحدد بشكل واضح ودقيق صور هذه الجرائم وإيجاد العقوبات الملائمة لها التي من شأنها تحقيق الردع العام والخاص. ولا بد من توسع المشرع الجزائي في مفهوم المال بحيث يشمل كل شيء ينطوي على قيمة. حيث أن أي تأخير من جانب المشرع في مباشرة هذه

المسؤولية من شأنه أن يصيب المصالح العامة والخاصة بالخطر وأن يفسح المجال واسعاً للمجرمين في استغلال الثغرات القانونية القائمة في النظام القانوني.

- ضرورة زيادة الوعي لدى المواطنين بمفهوم الحكومة الالكترونية وإحاطة هذا المشروع الرائد بالضمانات القانونية الكافية التي تكفل حمايته بالإضافة إلى إحاطته بإجراءات أمنية الكترونية تمنع استغلاله و اختراقه من قبل مجرمي المعلوماتية لغاية وقائية الهدف منها منع الجريمة قبل وقوعها.
- ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية الالكترونية وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم كلّها وتبين كذلك الاختصاص المكاني في حال وقوعها وكيفية تسليم مجرمي المعلوماتية وغير ذلك من الأمور، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم المعلوماتية.
- إعطاء دورات متخصصة في الجرائم المعلوماتية لأفراد الضابطة العدلية وللقضاة حتى يكونوا على معرفة بطبيعة هذه الجرائم وأساليب ارتكابها، ومن الأفضل إحالة الجرائم المعلوماتية إلى قضاء متخصص مؤهل للتعامل مع هذه الجرائم والفصل فيها.
- تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد القضائية وكذلك في الكليات الشرطية.

تم بحمد الله وتوفيقه

المراجع

- أحمد، هلالي عبد اللاه، (1997). **التزام الشاهد بالإعلام في الجرائم المعلوماتية.** (ط1). القاهرة: دار النهضة العربية.
- أحمد، هلالي عبد اللاه، (2003). **الجوانب الموضوعية والاجرائية لجرائم المعلوماتية.** (ط1). القاهرة: دار النهضة العربية.
- الأباصيري، فاروق محمد، (2002). **عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت.** (ط1). بيروت: الدار الجامعية للنشر.
- اتليسك، جين، (1994). **كل شئ عن الحواسيب** (ترجمة مركز التعريب والترجمة). (ط1). بيروت: الدار الجامعية للنشر.
- بحر، ممدوح خليل، (1983). **حماية الحياة الخاصة في القانون الجنائي.** (ط1) القاهرة: دار النهضة العربية.
- تمام، أحمد حسام طه، (2000). **الجرائم الناشئة عن استخدام الحاسب الآلي.** (ط1). القاهرة: دار النهضة العربية.
- حجازي، عبد الفتاح بيومي، (2002). **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت.** (ط1). القاهرة: دار الكتب القانونية.
- حجازي، عبد الفتاح بيومي، (2002). **الأحداث والإنترنت.** (ط1). الإسكندرية: دار الفكر الجامعي.
- حجازي، عبد الفتاح بيومي، (2002). **النظام القانوني لحماية التجارة الالكترونية** (الكتاب الثاني). (ط1). الإسكندرية: دار الفكر الجامعي.
- حسبو، عمرو أحمد، (2000). **حماية الحريات في مواجهة نظم المعلومات.** (ط1). القاهرة: دار النهضة العربية.
- الحفناوي، فاروق علي، (2001). **موسوعة قانون الكمبيوتر ونظم المعلومات.** (ط1). القاهرة: دار الكتاب الحديث.

- حسني، محمود نجيب، (1969). **جرائم الاعتداء على الأموال**. (ط1) دون ناشر.
- الحسيني، عمر الفاروق، (1995). **المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية**. (ط2). القاهرة: دار النهضة العربية.
- حسين، محمد عبد الظاهر، (2002).**المسؤولية القانونية في مجال شبكات الإنترنت** (ط1). بدون ناشر.
- الداودي، غالب علي، (1999). **المدخل إلى علم القانون**. (ط6). عمان: دار وائل للطباعة والنشر.
- الدريني، محمد. (1961). **مقدمة في أساسيات الحاسوب**. (ط1). الرياض: معهد الإدارة العامة.
- رباح، غسان، (2001). **قانون الملكية الفكرية والفنية الجديد مع دراسة مقارنة حول الجرائم المعلوماتية**. (ط1). بيروت: دار نوفل .
- رستم، هشام محمد فريد، (1994). **الجوانب الإجرائية للجرائم المعلوماتية**. (ط1). أسيوط: مكتبة الآلات الحديثة.
- رمضان، مدحت، (2000). **جرائم الاعتداء على الأشخاص والإنترنت**. (ط1). الاسكندرية: دار المطبوعات الجامعية.
- الرومي، محمد أمين، (2003). **جرائم الكمبيوتر والإنترنت**. (ط1) القاهرة: دار النهضة العربية.
- الزعبي، محمد والشرايعة، أحمد وقطيشات، منيب والفارس، سهير والزعبي، خالدة، (2002). **الحاسوب والبرمجيات الجاهزة**. (ط5). عمان: دار وائل للنشر والتوزيع.
- الزيدي، وليد، (2003). **القرصنة على الإنترنت والحاسوب**. (ط1) عمان: دار أسامة للنشر والتوزيع.
- السعيد، كامل، (1997). **شرح قانون العقوبات (الجرائم المضرة بالمصلحة العامة)** (ط1) دون ناشر.

- السعيد، كامل، (1983). **شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن.** (ط2). عمان: دار الفكر للنشر والتوزيع.
- شتا، محمد محمد، (2001). **فكرة الحماية الجنائية لبرامج الحاسب الآلي.** (ط1). القاهرة: دار الجامعة الجديدة للنشر.
- شلباية، مراد، وفاروق، علي، (2001). **مقدمة إلى الإنترنت.** (ط1) عمان: دار المسيرة للنشر.
- الشوا، سامي، (1994). **ثورة المعلومات وانعكاساتها على قانون العقوبات.** (ط1). القاهرة: دار النهضة العربية.
- الشوابكة، محمد أمين، (2004). **جرائم الحاسوب والإنترنت.** (ط1) عمان: دار الثقافة للنشر والتوزيع.
- صالح، نائل عبد الرحمن، (1995). **محاضرات في قانون العقوبات الأردني، (القسم العام).** (ط1). عمان: دار الفكر للطباعة والنشر.
- الصغير، جميل عبد الباقي، (1992). **الجرائم الناشئة عن استخدام الحاسب الآلي.** (ط1). القاهرة: دار النهضة العربية.
- الصمادي، حازم نعيم، (2003). **المسؤولية في العمليات المصرفية الإلكترونية.** (ط 1). عمان: دار وائل للنشر.
- العاني، عادل ، (1995). **جرائم الاعتداء على الأموال في قانون العقوبات الأردني.** (ط1). عمان: دار الثقافة للنشر والتوزيع.
- عبده، نديم، (1991). **أمن الكمبيوتر (الفيروسات والقرصنة المعلوماتية وانعكاسها على الأمن القومي).** (ط1). بيروت: دار الفكر للأبحاث والدراسات.
- عرب، يونس، (2002)، **دليل أمن المعلومات والخصوصية (الجزء الأول) جرائم الكمبيوتر والإنترنت.** (ط 1). بيروت: اتحاد المصارف العربية.
- عرب، يونس، (2001). **قانون الكمبيوتر.** (ط1). بيروت: منشورات اتحاد المصارف العربية.

- عفيفي، عفيفي كامل، (200). **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية.** (ط1). بدون ناشر.
- الغريب، انتصار نوري، (1994)، **أمن الكمبيوتر والقانون.** (ط1) بيروت: دار الراتب الجامعية.
- فوريستر، توم، (1989). **مجتمع التقنية العالية** (ترجمة محمد كامل عبد العزيز). (ط1). عمان: مركز الكتب الأردني.
- القاضي، زياد ، (1997). **أساسيات علم الحاسوب.** (ط1). عمان: دار صفاء للنشر والتوزيع.
- القاضي، زياد والقاضي، قصي واللحام، علي ومحمود ، سالم و مجدلاوي، يوسف ، (2000). **مقدمة إلى الإنترنت.** (ط1). عمان: دار صفاء للنشر والتوزيع.
- قايد ، أسامة عبد الله، (1988). **الحماية الجنائية للحياة الخاصة وبنوك المعلومات.** (ط1). بدون ناشر.
- قشقوش، هدى، (1992). **جرائم الحاسب الإلكتروني في التشريع المقارن.** (ط1). القاهرة: دار النهضة العربية.
- قورة، نائلة ، (2004، 2003). **جرائم الحاسب الاقتصادية.** (ط1). القاهرة: دار النهضة العربية.
- لطفي، محمد حسام، (1987). **الحماية القانونية لبرامج الحاسب الإلكتروني.** (ط1). القاهرة: دار الثقافة للطباعة والنشر.
- محمود ، عبد الله حسين، (2002). **سرقة المعلومات المخزنة في الحاسب الآلي.** (ط2). القاهرة: دار النهضة العربية.
- نجم، محمد وصالح، نائل عبد الرحمن، (1999). **قانون العقوبات الأردني (القسم الخاص).** (ط1) دون ناشر.
- النقري، معن، (2001). **المعلوماتية والمجتمع.** (ط1). الدار البيضاء: المركز الثقافي العربي.

- مغبغب، نعيم، (1998). **مخاطر المعلوماتية والإنترنت**. بيروت: منشورات الحلبي الحقوقية.
- المناعسة، اسامة والزعبي، جلال والهواوشة، صايل، (2001). **جرائم الحاسب الالي والإنترنت**. (ط1). عمان: دار وائل للنشر.
- منصور، عوض، (1986). **برمجة الحاسبات الإلكترونية بلغة بيسك**. (ط1). القاهرة: دار الجامعة الجديدة.
- منصور، محمد حسين، (2003). **المسؤولية الالكترونية**. (ط1). القاهرة: دار النهضة العربية.
- الهيتي، محمد حماد، (2004). **التكنولوجيا الحديثة والقانون الجنائي**. (ط1). عمان: دار الثقافة للنشر والتوزيع.
- هونيكوت، جيري، (1997). **مبادئ الإنترنت** (ترجمة عمر الأيوبي)، (ط1) بيروت: أكاديمياً.

الرسائل الجامعية:

- العزام، أحمد حسين، (2001). **الحكومة الإلكترونية في الأردن: إمكانيات التطبيق**، رسالة ماجستير، غير منشورة، جامعة اليرموك، إربد، الأردن.
- عرب، يونس ، (1994). **جرائم الحاسوب: دراسة مقارنة**، رسالة ماجستير، غير منشورة، الجامعة الأردنية، عمان، الأردن.

الأبحاث العلمية

- Ulrich Sieber، (1993). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. بحث مقدم إلى **المؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة، اكتوبر (25- 28).
- البياتي، هلال، (1998). استخدام الحاسبات الفنية وحمايتها. **بحث مقدم إلى ندوة القانون والحاسوب**، المنعقد في العراق، بغداد، .

- دلالعة، سامر، (2004). الحماية الجنائية لبرنامج الحاسوب. **بحث مقدم إلى مؤتمر القانون والحاسوب**، المنعقد في جامعة اليرموك، إربد، في الفترة من (12 – 14) تموز.
- السعدي، واثبة، (2004). الحماية الجنائية لمعلومات وبرامج الحاسوب. **بحث مقدم الى مؤتمر القانون والحاسوب**، المنعقد في جامعة اليرموك، إربد، في الفترة من (12 – 14) تموز.
- السعيد، كامل، (1993). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. **بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي**، القاهرة، الفترة من (25- 28) أكتوبر.
- شحاتة، علاء الدين، (1993). رؤيا أمنية للجرائم الناشئة عن استخدام الحاسب الآلي. **بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة في الفترة من (25- 28) أكتوبر.
- الشوا، سامي، (1993). الغش المعلوماتي كظاهرة إجرامية مستحدثة. **بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة، الفترة (25- 28) أكتوبر.
- صالح، نائل عبد الرحمن، (2000). واقع جرائم الحاسوب في التشريع الجزائي الأردني. **بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت**، المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة.
- عبابنة، محمود، (2004). الحماية الجنائية لمعلومات وبرامج الحاسب الالي. **بحث مقدم الى مؤتمر القانون والحاسوب**، المنعقد في جامعة اليرموك، اربد، في الفترة من (12 –14) تموز.
- العقاد، محمد، (1993). جريمة التزوير في المحررات للحاسب الآلي. **بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة في الفترة من (25- 28) أكتوبر.

- عميش، رحاب، (2004). مشكلات الحماية الجنائية لبرامج الحاسب الآلي في قانون العقوبات الليبي. **بحث مقدم إلى مؤتمر القانون والحاسوب**، المنعقد في جامعة اليرموك، إربد، في الفترة من (12 –14) تموز.
- عوض، محمد محيي الدين، (1993). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات. **بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة في الفترة من (25 ـ28) أكتوبر.
- غالي، عبد الكريم، (2001). الحماية الجنائية للمعلومات على ضوء القانون المغربي. **بحث مقدم إلى مؤتمر الوقاية من الجريمة في عصر العولمة**، المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة وبالتعاون مع أكاديمية نايف العربية للعلوم الأمنية، في الفترة من (6 ـ8) مايو.
- الفخري، عوني، (1998). المسؤولية المدنية الناشئة عن استعمال الحاسوب. **بحث مقدم إلى ندوة القانون والحاسوب**، المنعقدة في العراق، بغداد.
- القبائلي، سعد حماد، (2004). ضوابط الحماية الإجرائية لبرامج الحاسب الآلي. **بحث مقدم إلى مؤتمر القانون والحاسوب**، المنعقد في جامعة اليرموك، في الفترة من (26- 27).
- قندح، خليل، (2004). الجرائم المرتكبة بواسطة المعلوماتية. **بحث مقدم إلى مؤتمر القانون والحاسوب**، المنعقد في جامعة اليرموك، إربد، الفترة من (12 ـ14) تموز.
- قشقوش، هدى، (1993). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. **بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة الفترة من (25 ـ28) أكتوبر.
- لطفي، محمد حسام، (1993). الجرائم التي تقع على الحاسبات أو بواسطتها. **بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي**، المنعقد في القاهرة الفترة من (25 ـ28) أكتوبر.

- لطفي، محمد حسام، (1991). الحماية القانونية لبرامج الحاسب. **بحث منشور ضمن كتاب الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف**، بيروت: اتحاد المصارف العربية.
- المرزوقي، محمود محمد حسن، (2002). جرائم الحاسب الآلي. **بحث منشور في المجلة العربية للفقه والقضاء التي تصدر عن الأمانة العامة لجامعة الدول العربية**، العدد الثامن والعشرون.

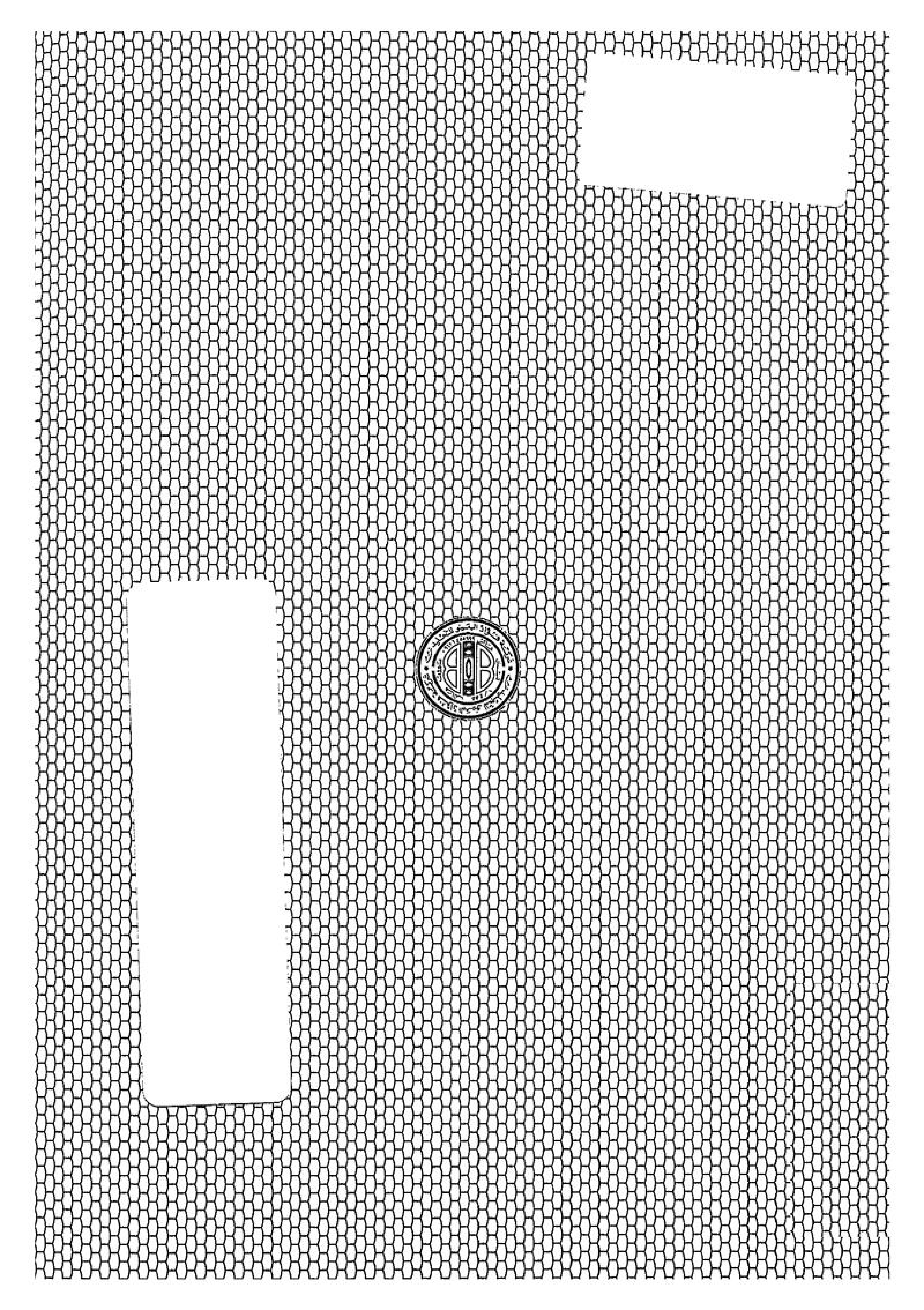
الدوريات:

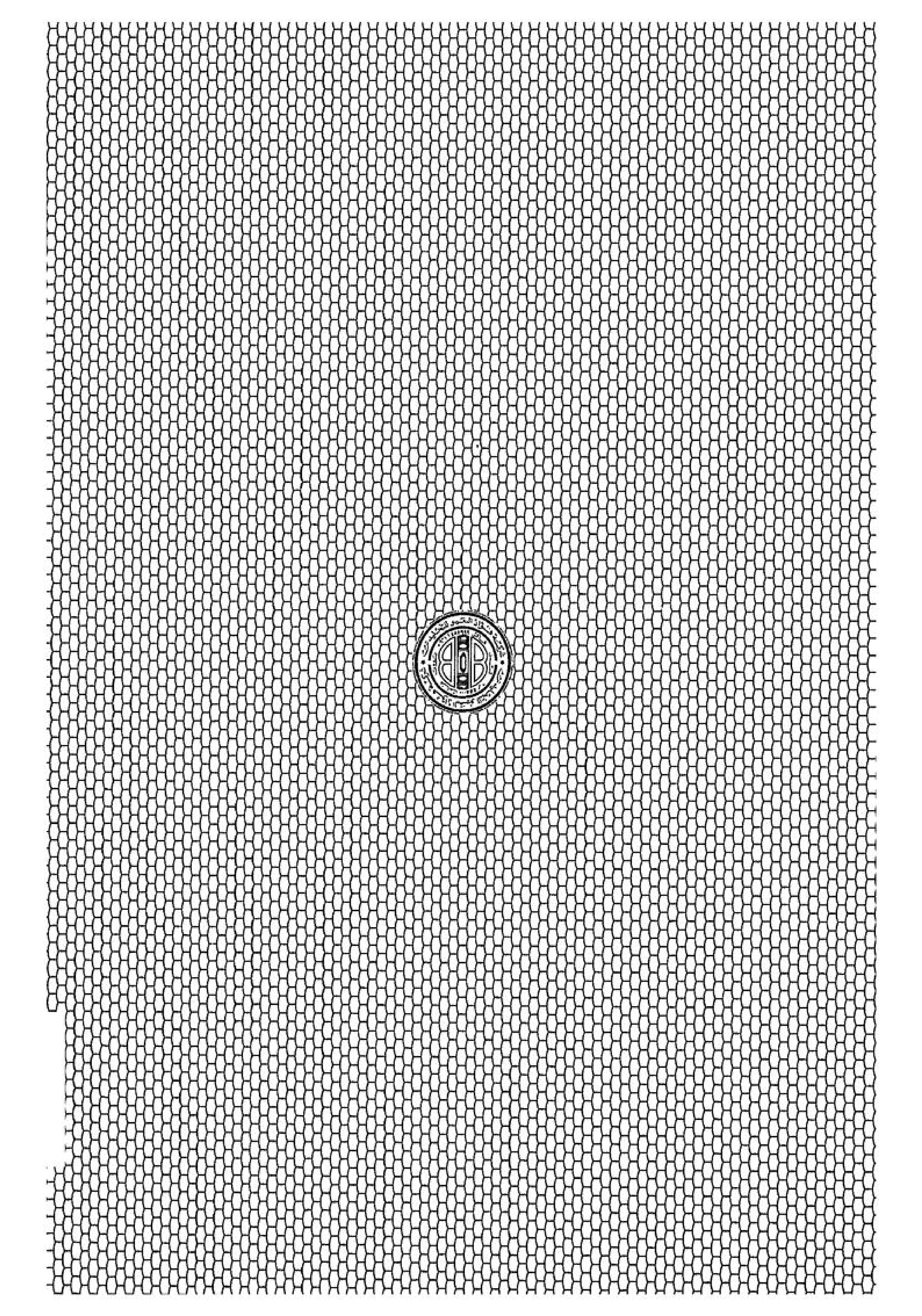
- أبرز المصطلحات التقنية المستعملة في تطبيقات شبكة الإنترنت، (1995). **مجلة الكمبيوتر والاتصالات والإلكترونيات**. المجلد (12). العدد (7). بيروت: دار الصياد انترناشونال.
- أكرم عيسى، أنواع جرائم الحاسوب. **جريدة الدستور**، عمان، عدد (11091) بتاريخ (2001/1/20).
- بطرس، أنطوان، (1992) المعلومات وأهميتها في العصر الحديث. **مجلة الكمبيوتر والاتصالات والإلكترونيات**. المجلد الثامن ، العدد (12). بيروت: دار الصياد انترناشونال.
- التصنت على الاتصالات التي تعتمد الرقمية، (1995). **مجلة الكمبيوتر والاتصالات والإلكترونيات**. المجلد (12) العدد (7). بيروت: دار الصياد انترناشونال.
- رستم، هشام محمد فريد، (1995). جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة. **مجلة الدراسات القانونية**. العدد السابع عشر. القاهرة.
- رضوان، رضا عبد الحكيم، سبتمبر (1999). التقنيات العلمية الحديثة في مكافحة فيروسات الكمبيوتر: **مجلة الأمن والحياة**، تصدر عن أكاديمية نايف العربية للعلوم الأمنية، السعودية، العدد (204).

- غرير، ايرل، (1998). أنا فيروس، فهل تسمع زئيري. **مجلة بايت**. العدد (3) السنة الرابعة.
- الكساسبة، فهد يوسف، يوليو (2001). التطور التقني وتطور الجريمة. **مجلة الأمن والحياة**، تصدر عن أكاديمية نايف العربية للعلوم الأمنية، السعودية. العدد (227).
- مستقبل صناعة تقنية المعلومات في دول مجلس التعاون الخليجي، (2003). ورقة عمل مقدمة إلى الأمانة الفنية لتقنية المعلومات بوزارة الاقتصاد الوطني في عمان لمؤتمر الصناعيين التابع لدول مجلس التعاون الخليجي. **مجلة الغرفة**. العدد (43).
- محمد، سليمان مصطفى، مارس (1999). جرائم الحاسوب وأساليب مواجهتها، **مجلة الأمن والحياة**، تصدر عن أكاديمية نايف العربية للعلوم الأمنية، السعودية. العدد (199).
- محمد، عادل عبد الجواد، ديسمبر (2001). إجرام الإنترنت. **مجلة الأمن والحياة**، تصدر عن أكاديمية نايف العربية للعلوم الأمنية، السعودية، العدد (221).

المواقع الإلكترونية على الشبكة العالمية للمعلومات (الإنترنت):

- www.Aljazeera.net.science-tech/2003
- www.News.BBC.co.uk/Hi/Arabic/Newsid/
- www.Arabicn.net/Arabic/Nadweh/Pivot-7/Arabic-Arrangement/HTM
- www.Alwatan.com
- www.Alyasser.gov.SA
- Http://USINFO.state.gov/journals/itgic/0801/ijga/comntry3.htm
- www.Habtoor.com
- www.Alrivadh.com.SA/contents/19-05-2003/rivadhnet/cov
- www.Minshawi.com/old/internetcrime-in/20the20%law.htm
- www.annabaa.org/nbsnews/14134.htm
- www.gn4me.com/eteslat/article.JSP?art =3299
- www.albayan.co.ae/albayan/2001/09/04/mnw/13.htm
- www.gn4me.com/etesalat/article.jsp?art-id =7432









تصميم وإخراج/ مكتب دار الثقافة للتصميم والإنتاج

